NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF THE ARMY'S TACTICAL PACKET NETWORK

by

Earnest E. Hansley

June 1996

Principal Advisor: Gilbert M. Lundy
Associate Advisor: Orin E. Marvel

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
June 1996

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE AN ANALYSIS OF THE ARMY'S TACTICAL PACKET NETWORK

5. FUNDING NUMBERS

6. AUTHOR(S) Earnest E. Hansley

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

This thesis represents an analysis of the U.S. Army's Tactical Communications System with particular emphasis on the Tactical Packet Network (TPN). It is a study of the Army's TPN and the proposed upgrade solutions. The U.S. Army awarded GTE a contract to replace the TPN Exterior Gateway Protocol with the Border Gateway Protocol. Additionally, the U.S. Army intends to upgrade the bandwidth of the Small Extension Node Switch and the Node Center Switch. The goal of both upgrades is to enhance the TPN.

One cannot look at TPN without looking at the overall infrastructure or the Army Tactical Command and Control System (ATCCS). Even this view is shortsighted. The ATCCS continues to evolve to meet the information requirements of the warfighter. Thus, a fair study must include our current capabilities and our future intentions for C4I. This thesis analyzes both.

14. SUBJECT TERMS Tactical Packet Network (TPN), Army Tactical Command and Control System (ATCCS), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP)

15. NUMBER OF PAGES 98

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

AN ANALYSIS OF THE ARMY'S TACTICAL PACKET NETWORK

Earnest E. Hansley
Captain, United States Army
B.S., Fort Valley State College, 1985

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE
IN
SYSTEMS TECHNOLOGY
[Command, Control, and Communications (C3)]

from the

NAVAL POSTGRADUATE SCHOOL
June 1996

Author: Earnest E. Hansley
Earnest E. Hansley

Approved by:
Gilbert M. Lundy, Principal Advisor

Orin E. Marvel
Orin E. Marvel, Associate Advisor

Dan C Boger
Dan C. Boger, Chairman
Command, Control & Communications (C3) Academic Group

ABSTRACT

This thesis represents an analysis of the U.S. Army's Tactical Communications System with particular emphasis on the Tactical Packet Network (TPN). It is a study of the Army's TPN and the proposed upgrade solutions. The U.S. Army awarded GTE a contract to replace the TPN Exterior Gateway Protocol with the Border Gateway Protocol. Additionally, the U.S. Army intends to upgrade the bandwidth of the Small Extension Node Switch and the Node Center Switch. The goal of both upgrades is to enhance the TPN.

One cannot look at TPN without looking at the overall infrastructure or the Army Tactical Command and Control System (ATCCS). Even this view is shortsighted. The ATCCS continues to evolve to meet the information requirements of the warfighter. Thus, a fair study must include our current capabilities and our future intentions for C4I. This thesis analyzes both.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1

B. PURPOSE 2

C. SCOPE 3

II. COMBAT COMMUNICATIONS AT ECHELONS CORPS AND BELOW 5

A. INTRODUCTION 5

B. THE ARMY TACTICAL COMMAND AND CONTROL SYSTEM 5

C. BATTLEFIELD FUNCTIONAL AREAS 6

1. Maneuver Control System (MCS) 7

2. Advanced Field Artillery Tactical Data System (AFATDS) 7

3. Forward Area Air Defense Command, Control, Communications and Intelligence (FAADC3I) 7

4. All Source Analysis System (ASAS) 7

5. Combat Service Support Control System (CSSCS) 8

D. AREA COMMON USER SYSTEM (ACUS) 8

1. Subscriber Terminals 9

2. Subscriber Access 9

E. MOBILE SUBSCRIBER EQUIPMENT (MSE) 9

1. Introduction 9

2. What is MSE? 9

3. Network Features 10

4. MSE Deployment 10

5. Division Network 11
6. Node Center Switch (NCS) 11
7. Large Extension Node (LEN) 11
8. Small Extension Node (SEN) 13
9. Radio Access Unit (RAU) 13
10. Subscriber Equipment 15
F. CONCLUSION 15

III. PACKET SWITCHING CONCEPTS 21
A. INTRODUCTION 21
B. PACKET SWITCHING 21
1. Types of Switching 21
2. What is Packet Switching? 22
3. History of Packet Switching 22
4. Packet Switching Advantages and Disadvantages 23
5. Packet Network Induced Errors 24
6. Packet Switching Overhead 27
C. OPEN SYSTEMS 28
1. Open Systems Interconnection (OSI) 28
2. The OSI Seven-Layer Model 29
D. CONCLUSION 31

IV. THE TACTICAL PACKET NETWORK 33
A. INTRODUCTION 33
B. THE TPN STRUCTURE 33
1. What is TPN? 33

2. Simple TPN Deployment 33
3. Complex TPN Deployment 33
4. MSE Packet Network Deployment 35
5. TPN Equipment 35
C. PACKET SWITCHING AND ROUTING 36
D. TPN PROTOCOLS 36
1. The DoD Protocol Layers 36
2. Application Layer 37
3. Transmission Control Protocol/Internet Protocol (TCP/IP) 38
4. Transport Layer 39
5. Network Layer 39
E. MESSAGING WITH TPN AND THE TPN MTA 39
1. Node Center Switch Message Transfer Agent 39
2. Sendmail 40
F. THE TPN TACTICAL NAME SERVER (TNS) 40
1. What is TNS? 40
2. The TNS Domain 40
3. TNS Functions 41
4. TNS Databases 41
G. CONCLUSION 42
V. TACTICAL PACKET NETWORK ISSUES 43
A. INTRODUCTION 43
B. SOFTWARE 43
1. Internodal Trunk Markings 43
2. Duplicate PSNs 44

3. Exchange Processes Dying 44
4. TNS Registration Utility 44
5. Node Switch Lookup (NSLookup) 44
6. Registration Processes Dying 45
C. INTEROPERABILITY 45
1. TPN versus DMS Protocols 45
2. Interoperability Solutions 46
D. THROUGHPUT 48
1. Units Report Bandwidth Problems 48
2. LAN Applications Impact Wide Area Network 48
3. Documents Impact Bandwidth 49
4. Network Operations Affect Throughput 49
5. Quickfix Bandwidth Solutions 49
6. Information Management Schedule Imposed 49
E. SECURITY 50
F. GATEWAY PROTOCOLS 50
1. Introduction 50
2. Exterior Gateway Protocol 51
G. BORDER GATEWAY PROTOCOL 55
1. Introduction 55
2. BGP Efficiency 56
3. BGP Message Format 56
4. The OPEN Message 57
5. The KEEPALIVE Message 57
6. The NOTIFICATION Message 57
7. The UPDATE Message 58

H. COMPARISON OF BGP AND EGP 59

VI. EVOLVING COMMUNICATIONS REQUIREMENTS 61
A. THE NEW STAGE 61
B. PLANNING FOR JOINT CHALLENGES 61
C. PRINCIPLES OF PLANNING 62
1. Interoperablility 63
2. Discipline 63
3. Economy 63
4. Flexibility 64
5. Security 64
6. Reliability 64
7. Survivability 64
8. Timeliness 64
9. Combined Operations 65
D. THE FUTURE PATH 65
1. The Army Enterprise Strategy 66
2. Warfighter Information Network (WIN) 67
3. Conclusion 69

VII. CONCLUSION 71
A. INTRODUCTION 71
B. THESIS RESULTS 71
C. FURTHER RESEARCH 72

LIST OF REFERENCES 73

INITIAL DISTRIBUTION LIST 75

LIST OF FIGURES

1. ATCCS Objective Architecture 6
2. MSE Deployment ~ 42 Nodes 11
3. Division Network 12
4. Node Center Switch (NCS) 12
5. Large Extension Node (LEN) 13
6. Small Extension Node (SEN) 14
7. Radio Access Unit (RAU) 14
8. Digital Non-secure Voice Terminal (DNVT) 16
9. Secure Voice Telephone (DSVT) 17
10. Communication Terminal (CT, AN/UGC-144) 18
11. Mobile Subscribers Radio Telephone (MSRT) 19
12. A Packet Switching Network used for Voice Communication 23
13. Basic Operation of a Packet Switched Network: Movement of Three-packet Message from User A to User B 26
14. Basic Operation of a Packet Switched Network with a Switch Failure: Loss of a Packet 26
15. Basic Operation of a Packet Switched Network with a Line Failure: Duplication of a Packet 27
16. Single MSE Packet Switch Network 34
17. Internetwork of Networks 34
18. ECB Communication System 35
19. Some Protocols Used Within TPN 37
20. Exterior Gateway Protocol (EGP) 51
21. EGP Messages 52
22. Fixed Header of EGP Messages 53
23. Network Reachability Information 55

24. Message Header Format 56
25. BGP Header 58

LIST OF TABLES

1. Highlights of Current EGP Approach 60

2. Services Provided 62

3. Shifting Paradigms 68

EXECUTIVE SUMMARY

The purpose of this thesis is to analyze the U.S. Army's Tactical Packet Network (TPN). There are already proposed changes and approved solutions. GTE proposed changing the gateway protocol from Exterior Gateway Protocol (EGP) to Border Gateway Protocol version 4 (BGP-4). A key question to ponder is whether these solutions represent a near-term fix or long-term solutions. Equally significant is the consideration of where the Army is now in terms of communications capabilities and what are the future plans. This thesis represents an attempt to answer these questions. It is constructed in a logical manner to facilitate reading. Based on the level of individual background knowledge about the topic, the reader can skip to the chapter he or she is interested in.

The progression of topics is as follows. First, the background represents an overview and scope that sets the stage for subsequent topics. Secondly, the Army Tactical Command and Control System reflects not only the current tactical communications architecture, but facilitates understanding the system that TPN traverses. Additionally, it provides information regarding where the Army is now and where it is going in the near-term.

The middle three chapters are designed to describe packet switching from concepts to reality. Chapter III discusses packet switching technology, which is followed by the Tactical Packet Network. The aim of the chapter on the TPN is to provide adequate background information regarding not only TPN functions, but equipment too. Armed with an understanding of the communications system, packet switching, and the TPN, a reader can better appreciate and relate to the TPN issues and solutions.

Part of this research involved scrutinizing a multitude of TPN-related after-action reports (AARs) from exercises conducted during and after the fielding of TPN. It also involved a detailed review of studies conducted by GTE and DOD agencies regarding TPN challenges and solutions. A substantial amount of time was also spent researching the various technology applications chosen, i.e., TCP-IP, EGP, BGP-4, and multi-level security.

This thesis concludes with the realization that the GTE proposal is the best solution to resolve the current TPN shortfalls. The plan takes advantage of the latest gateway protocol technology and is somewhat far-sighted in that it addresses the anticipated interoperability issue regarding the Defense Messaging System (DMS) and TPN. However, the proposal is not the optimal solution. The best solution is one that capitalizes on the latest equipment too, which is easier said than done. Additionally, there are multi-level security issues that must be resolved.

The future direction of the U.S. Army is already promulgated in the Army Enterprise Strategy and TRADOC Pamphlet 525-5 (Force XXI Operations). The Enterprise Strategy is parsed into two publications: "The Vision" and "The Implementation Plan". This strategy reflects a Total Quality Management (TQM) approach for meeting future requirements. TRADOC Pamphlet 525-5 is the baseline approach for twenty-first century operations. The framework is established; now the work must be performed. This too is easier said than done.

The key is to have a feasible plan to meet today's challenges and a long-range plan to meet tomorrow's requirements. The TPN plan is feasible. The Army Enterprise Strategy and Force XXI represent a long view in a world of uncertainty. Both plans are sound and workable, unless budgetary constraints hinder their progress.

LIST OF ACRONYMS

AC	Alternating Current Power
ACUS	Area Common User System
ADA	Air Defense Artillery
ADDS	Army Data Distribution System
AFATDS	Advanced Field Artillery Tactical Data System
ALB	Air Land Battle
ANSI	American National Standards Institute
AR 94	Atlantic Resolve 94
ARP	Address Routing Protocol
AS	Autonomous System
ASAS	All Source Analysis System
ASCII	American Standard Code for Information Interchange
ATCCS	Army Tactical Command and Control System
ATM	Asynchronous Transfer Mode
AUTODIN	Automated Digital Network
BER	Bit Error Rates
BFACS	Battlefield Functional Area Control System
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol Version 4
BIND	Berkeley Internet Domain
BSI	British Standards Institution
C2	Command and Control
C3	Command, Control & Communication
C4	Command, Control, Communications And Computers
CCITT	Consultative Committee for International Telephony and Telegraphy
CE	Communications-Electronics Systems
CECOM	Communications Electronic Command

CLDAP	Connectionless Lightweight Directory Access Protocol
CNR	Combat Net Radio
CNRI	Combat Net Radio Interface
COMSEC	Communication Security
COSCOM	Corps Support Command
CP	Command Post
CSA	Chief of Staff , U.S. Army
CSS	Combat Service Support
CSSCS	Combat Service Support Control System
CT, AN/UGC-144	Communication Terminal
CTs	Communications Terminals
DAP	Directory Access Protocol
DC	Direct Current
DCD	Directorate of Combat Development
DDN	Defense Data Network
DIB	Directory Information Base
DISCOM	Division Support Command
DMS	Defense Message System
DNVT	Digital Non-secure Voice Terminal
DoD	Department of Defense
DSA	Directory System Agent
DSN	Defense Switched Network
DSVT	Secure Voice Telephone
DTG	Digital Trunk Group
E3	End-To-End Encryption
EAC	Echelons Above Corps
ECB	Echelons Corps and Below
EGP	Exterior Gateway Protocol
FAADC3I	Forward Area Air Defense Command, Control, Communications and Intelligence

FLC-SW	Force Level Control Software
FM	Frequency Modulation
FSEN	Future SEN
ICMP	Internet Control Message Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
JTF	Joint Task Force
LAN	Local Area Network
LDFs	Lightweight Digital Facsimiles
LEN	Large Extension Node
LOS	Line-Of-Sight
MCS	Maneuver Control System
MFG	Multi-Function Gateway
MPN	MSE Packet Network
MS	Microsoft
MSE	Mobile Subscriber Equipment
MSRT	Mobile Subscribers Radio Telephone
MTA	Mail Transfer Agent
MTA	Message Transfer Agent
NAK	Negative Acknowledgment
NATO	North Atlantic Treaty Organization
NC	Node Center
NCS MTA	Node Center Switch Message Transfer Agent
NCS	Node Center Switch
NES	Network Encryption System
NMC	Network Management Center
NOS	Network Operating System
OOTW	Operations Other Than War

OPSEC	Operations Security
ORD	Operational Requirement Document
OSI	Open Systems Interconnection
POTS	Portable Off the Shelf
PS	Packet Switch
RARP	Reverse Address Routing Protocol
RAU	Radio Access Unit
RAUs	Radio Access Units
RMA	Revolution in Military Affairs
SCC	Systems Control Center
SED	Software Engineering Division
SEN	Small Extension Node
SOAC	Signal Officer Advance Course
SOBC	Signal Officer Basic Course
SONET	Synchronous Optical Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TNS	Tactical Name Server
TPN	Tactical Packet Network
TQM	Total Quality Management
UA	User Agent
UDP	User Datagram Protocol
USASC&FG	The United States Army Signal Center and Fort Gordon
VTC	Video Teleconferencing
WAN	Wide Area Network
WIN	Warfighter Information Network

I. INTRODUCTION

A. BACKGROUND

In 1991, presidential candidate Bill Clinton pledged to restructure our military forces for a new era. The former Secretary of Defense (the late Les Aspin) revealed the restructuring plan in The Bottom Up Review. Secretary Aspin said, "We'll have a force based on tomorrow's requirements, a lean mobile, high-tech force ready to protect Americans against the real danger they face in this new era." [Ref. 1] Since then, the U. S. Army has not only restructured its force, but modified its vision as well. Visions such as Digitization of the Battlefield and the Tactical Internet that were once concepts are rapidly becoming reality as the U.S. Army postures itself for the twenty-first century.

A very vital part of the Tactical Internet is the Tactical Packet Network (TPN). The TPN involves using packet switching technology over MSE/TRITAC networks. Although the U.S. Army already completed its fielding of TPN, there are still issues that must be resolved. The challenge of bandwidth is constant, while the data requirements continue to increase. Equally significant, there are multilevel security issues that must be resolved. Key questions to ponder are can the TPN can fulfill future requirements as is or should it be upgraded? Should the U. S. Army purchase a new system altogether?

GTE is currently under contract to provide Border Gateway Protocol-4 (BGP-4) capability as an enhancement to the TPN. Additionally, GTE must increase the throughput of the Small Extension Node Switch and the Node Center Switch. These enhancements are upgrades to an existing system. The major question of whether the current or upgraded TPN system supports the army's vision is yet to be answered. The foundation for the U.S. Army future directional path is already established.

Historically, the major communication systems have been stovepipe systems that only exchange information with like systems. The Goldwater-Nichols Act shifted the military focus from that of a unique service orientation to a joint perspective. As such, our current and future systems must be interoperable across DoD. We have not yet reached that plateau. But, we could in the future, as the Information Age continues to revolutionize the way we conduct operations by bringing forth new ideas and new technologies. John Naisbitt, author of *Megatrends*, credited Daniel Bell as recognizing that in our new society, the strategic resource is information [Ref. 2]. Although his remarks were not directed at the military, they are applicable.

Over the years, the U.S. Army has made several doctrinal changes such as Airland Battle and now Force XXI that affect the way we communicate. In order to meet the challenges that doctrinal changes bring forth, the U.S. Army continues to modify some systems and procure others. Changes have affected manpower, too. We have experienced a major downsizing in the Army and other services. Supposedly it is not over yet. The one constant during the aforementioned transitions is the goal of communications, "Get the Message Through." Today, communications systems must still get the information from point to point. The speed of information flow remains critical because in some cases, old information is worst than no information. The requirement to provide rapid, reliable, and flexible communication is ever so significant as information requirements increase despite a reduction in forces.

Several years ago, the U.S. Army changed its Acquisition Strategy to take advantage of commercial products, provided they are cost-effective and feasible. The procurement of the packet switch is the first step of several that the Army must take to maintain its technological edge throughout the world. The TPN data capabilities fill a void that has existed since the U.S. Army fielded Mobile Subscriber Equipment (MSE). The commercial standards such as X.25 protocols and Transmission Control Protocol/Internet Protocol (TCP/IP) allow TPN to traverse different types of networks. Since it uses the existing MSE network, it facilitated the transition to TPN.

B. PURPOSE

The purpose of this thesis is to conduct an analysis of the Tactical Packet Network, commonly referred to as TPN. The TPN is a packet-switched network designed for a tactical environment. The system is an enhancement to the U.S. Army Communication

Architecture. It uses the existing Mobile Subscriber Equipment (MSE) network to pass data. There are a multitude of lessons learned from the fielding of TPN. Some issues have not yet been resolved. A major aim of this thesis is to consolidate as well as address some of the issues and solutions. Additionally, a principal goal of this thesis is to scrutinize some of the TPN solutions such as the transition from Exterior Gateway Protocol to Border Gateway Protocol. Based on an analysis of how the U.S. Army provides communications now and how it will communicate in the future, this thesis seeks to address whether the future path provides a framework for future communications that will meet the future needs of the warfighter.

C. SCOPE

The scope of this thesis is to analyze the U.S. Army tactical communications at Echelons Corps and Below (ECB). Also, it examines the U.S. Army's strategy to meet future requirements. The primary focus will be on the TPN and some of the issues and challenges associated with it. Requisites include looking at how the Army currently provides communications support at ECB, discussing some of the unique functional capabilities that provide the communication services, and how the U.S. Army intends to support the Warfighter in the future.

This document is organized into seven chapters. Chapter II is an analysis of combat communications at ECB. The emphasis is on the Army Tactical Command and Control System (ATCCS), the Battlefield Functional Areas (BFAs) and Mobile Subscriber Equipment. Chapter III discusses packet switching concepts, followed by the Tactical Packet Network in Chapter IV. Chapter V is a compilation of issues, solutions, and resolutions for the TPN. Chapter VI encapsulates evolving communications requirements and the framework for future communications based on emerging technologies. Chapter VII provides a conclusion and identifies two topics for further research.

II. COMBAT COMMUNICATIONS AT ECHELONS CORPS AND BELOW

A. INTRODUCTION

The Department of Defense defines command and control (C2) as the exercise of authority and direction by a purposely designated commander over assigned forces in the accomplishment of the mission [Ref. 3]. The Army Tactical Command and Control System (ATCCS), the Battle Field Functional Areas (BFAs), and Mobile Subscriber Equipment facilitate the C2 process in the United States Army. This chapter discusses these three areas because they are key to understanding how the Army provides communications at the tactical or ECB level.

B. THE ARMY TACTICAL COMMAND AND CONTROL SYSTEM

The ATCCS is a system that is designed to support command and control in both the operations other than war (OOTW) environment and combat. Army Field Manual 24-7 lists the elements as commander, staff, doctrine, procedures, and tools used to command and control forces on the tactical battlefield [Ref. 4]. The purpose of ATCCS is to provide the commander and his staff with the information they need to effectively plan, coordinate, control, and direct the battle [Ref. 4].

The system allows the commander and staff to accumulate masses of information from multiple sources to generate more complete and useful information. The ATCCS also facilitates processing information to analyze trends and enhances information exchange between battlefield headquarters. The commander and staff can use the information to develop courses of action.

Figure 1 depicts the ATCCS Objective Architecture. The rectangular boxes bordering the outer circle represent the BFAs. The four interleaved circles depict the communications system required to support the BFAs functions. The Force Level Control Software (FLC-SW) operates in each Battlefield Functional Area Control System (BFACS) and will support the maintenance of force status, monitoring of current situation, planning of force missions, and control of FLC information transactions. FM 24-7 explicitly details the management structure and responsibilities associated with ATCCS. The focus of this section and the subsequent section is restricted to the general characteristics of the BFACs.

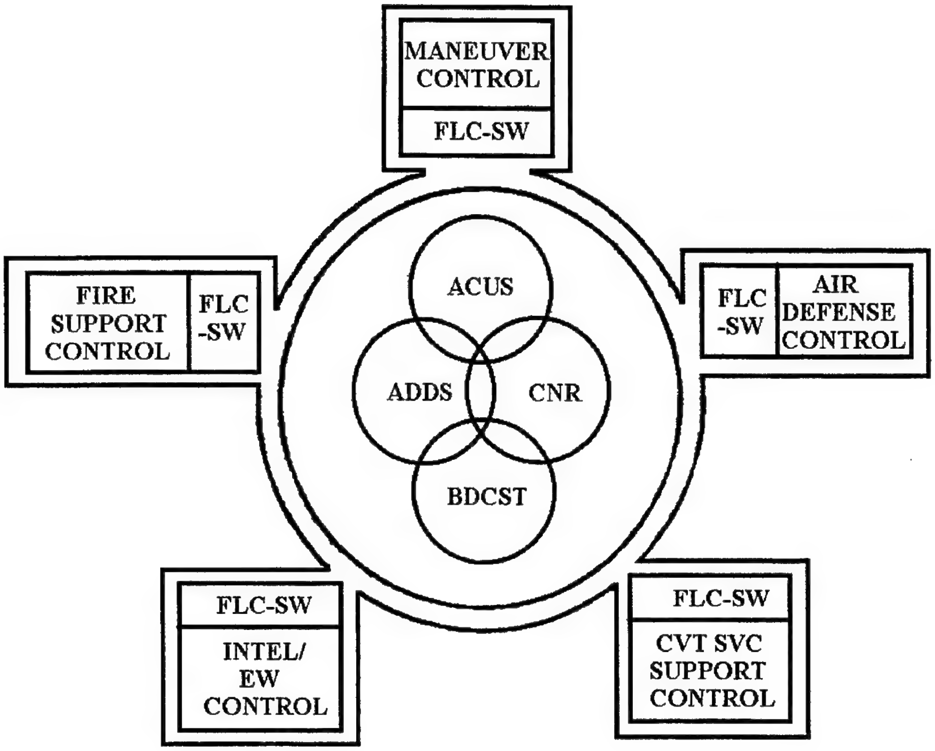


Figure 1. ATCCS Objective Architecture
From [Ref. 4, p. 2]

C. BATTLEFIELD FUNCTIONAL AREAS

The five BFAs are maneuver, fire support, air defense, intelligence and electronic warfare, and combat service support. Because each BFA is unique with different requirements, separate Battlefield Functional Area Control Systems have been developed. These systems enable the BFA commander and staff to synchronize and integrate the efforts of their subordinate elements to support the mission. The BFAs consistently exchange information to enhance synchronization.

1. Maneuver Control System (MCS)

The BFA system to support maneuvers is MCS. The MCS moves tactical information across the battlefield quickly, allowing the commander and staff to readily access information. The MCS will display current situation reports that provide enemy strength and movement, as well as the status of friendly forces. The commander also uses MCS to transmit critical battlefield information such as mission information, courses of action, schemes of maneuver, warning orders, priorities, intelligence requests and air operations requests. The MCS database will maintain and display in both text and graph formats, critical information on friendly and enemy forces. It also allows command posts (CPs) to view the same picture of the battlefield from battalion to corps.

2. Advanced Field Artillery Tactical Data System (AFATDS)

The BFA system for fire support is AFATDS. It is an integrated fire support C2 system that processes fire mission and other related information to coordinate and maximize the use of all fire support assets. Fire support assets include mortars, field artillery, attack helicopters, air support, naval gunfire, and offensive electronic warfare. Distributed processing capabilities allow fire missions to flow through the fire support chain where the target attack criteria will be satisfied by the most effective weapon system at the lowest level. The AFATDS automates and facilitates fire support planning and current operations.

3. Forward Area Air Defense Command, Control, Communications and Intelligence (FAADC3I)

The FAADC3I is the BFA system for air defense. It is an integrated system of weapons, sensors, and C2 designed to protect maneuver forces, critical CPs, combat support and combat service support elements from low-altitude air attack. The FAADC3I system, when fully fielded, will provide the Air Defense Artillery (ADA) commander with support for C2 of his elements across the battlefield and provide information needed to integrate air defense into the overall tactical plan.

4. All Source Analysis System (ASAS)

The ASAS is an integrated intelligence support system. It manages sensor and other resources; collects, processes and fuses intelligence data; stores, manipulates and displays this data; and expeditiously disseminates information by providing a common picture of enemy activity to all BFAs. The ASAS also provides the communications and intelligence capabilities that allow sensor and other intelligence data to automatically enter into databases and be simultaneously available at multiple analyst workstations. This automated process frees the analysts from manual processing and permits faster identification of information gaps and more efficient management of sensors to ensure proper coverage of target areas.

5. Combat Service Support Control System (CSSCS)

The BFA system for Combat Service Support (CSS), the CSSCS, is currently being fielded. The CSSCS aim is to consolidate and collate vast quantities of logistical data. Specifically, it will provide strategic and tactical commanders with timely, critical information on ammunition and fuel supplies, medical and personnel status, transportation, maintenance services, general supply and other field services. Additionally, the CSSCS will be fully operable with all other BFACs and provide C2 for the CSS commander's organic units.

D. AREA COMMON USER SYSTEM (ACUS)

The ATCCS has four categories of systems that facilitate the movement of information among the BFAs (see Figure 1). They are: ACUS, Army Data Distribution System (ADDS), Combat Net Radio (CNR), and Broadcast Systems. This section only focuses on ACUS because MSE is a component of the ACUS and TPN uses the MSE Network.

The ACUS is a seamless system that provides a means of secure, highly reliable voice and data, including packet communications for both mobile and static subscribers regardless of their location in Echelons Above Corps (EAC) or Echelons Corps and Below (ECB) areas of operation (ACUS) [Ref. 5] . At ECB, ACUS architecture is divided into seven functional areas. They are: 1) subscriber terminals, 2) mobile subscriber access, 3) wire subscriber access, 4) tactical packet network, 5) line-of-sight (LOS), 6) area coverage, and 7) system control.

1. Subscriber Terminals

Subscriber terminals are user-owned and operated equipment pieces that customers (subscribers) use to access the ACUS. The types of terminals include digital subscriber voice terminals (DSVTs), digital non-secure voice terminals (DNVT), lightweight digital facsimiles (LDFs), and communications terminals (CTs). Section E will provide further information regarding functionality.

2. Subscriber Access

The mobile subscriber gets access to the tactical communications network via Radio Access Units (RAUs) using their mobile subscriber radio telephone (MSRT). The wire subscriber obtains access to the communication system via Large Extension Node Switches (LENS) and Small Extension Node Switches (SENS). The RAUs, LENS, and SENS are all components of the Mobile Subscriber Equipment (MSE) Network.

E. MOBILE SUBSCRIBER EQUIPMENT (MSE)

1. Introduction

The post-Vietnam era resulted in monumental changes for the United States Army. One of the most significant changes was the introduction of Air Land Battle (ALB) Doctrine. The ALB Doctrine consists of four tenets: initiative, agility, depth, and synchronization. Field Manual 100-5 provides details regarding these tenets. Communications is key to achieving synchronization on the battlefield. Therefore, the implementation of ALB ultimately resulted in a change in the type of communications support provided. The signal support transitioned from simply an area support system to an area support system with mobile subscriber access. The MSE Communications Network, commonly referred to as MSE, is the communication support system resulting from doctrinal changes.

2. What is MSE?

The MSE Network is comprised of communication nodes called node centers that are linked by line-of-sight radios that enable area coverage via a tandem switched network. There is a Systems Control Center (SCC) that provides an automatic planning and management capability, including Network System Status. It is through MSE that the commander at ECB exercises command and control. MSE is the principal tactical common-user communication system at corps and division levels.

MSE is a circuit-switched, digital telecommunication system overlaid with a packet-switched network providing voice and data communications for a notional five division corps, covering an area of up to 37,500 square kilometers. The system is modern in that it provides users with features commonly available in commercial systems. It provides commanders and staff with telephone service, facsimile service, cellular phone service, data transmission service, and access to the combat net radio (CNR) network. MSE is referred to as a secret-high network because calls within the network are secure. Other MSE features include five precedence levels, voice conferencing capability, call-forwarding, and commercial network access.

3. Network Features

The MSE network is a 16 Kilobit per second (Kbps) digital network that is interoperable with North Atlantic Treaty Organization (NATO) systems and has a remote operating capability for command posts. The system uses a fixed directory that enables users to relocate to a different geographical location within the network area and use the same telephone number. Additionally, MSE is adaptable to outages. If the alternating current (AC) power is lost or shuts down, the system automatically reverts to its direct current (DC) backup power. The MSE system adds flexibility to deployments and enhances mobility.

4. MSE Deployment

Figure 2 is a representation of a fully deployed MSE Network. The shaded triangles depict communication nodes. The network is comprised of 42 nodes, 22 provided by the Signal Brigade and four by each of the five divisions. The network is extended from the Corps Rear to the rear of Divisional Maneuver Units. The area of coverage is 150 km by 250 km, which is 37,500 sq km or approximately 15,000 square miles.

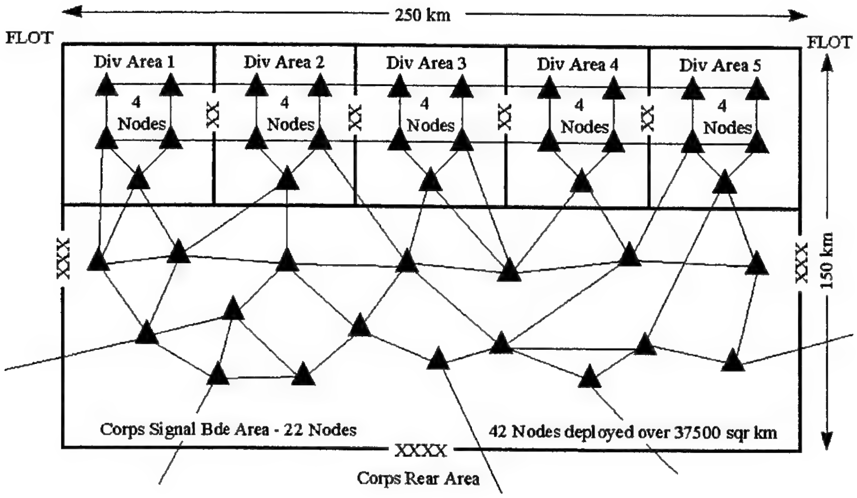


Figure 2. MSE Deployment ~ 42 Nodes

5. Division Network

Figure 3 is a layout of a division network. There are four node centers (NCs) in a division. They provide the backbone communications. The NCs communicate with SENs, LENs, RAUs, and other node centers to enable tandem switching. These MSE components will be discussed in subsequent sections.

6. Node Center Switch (NCS)

Figure 4 depicts the NC equipment pieces. The NCS will support 24 local subscribers and terminate up to 16 digital trunk groups. A digital trunk group is a switchboard to switchboard connection. The NCs will also provide tactical packet (TPN) connectivity for X.25 and 802.3 Local Area Network (LAN) subscribers. Additionally, the NCs can provide internodal connectivity to five node centers.

7. Large Extension Node (LEN)

Figure 5 is a representation of the LEN. The LEN supports heavily populated areas such as Division Support Command (DISCOM), Corps Support Command (COSCOM) and Corps Main Headquarters command post. It can support 164 digital subscribers and provide TPN connectivity for X.25 and 802.3 LAN subscribers. Additionally, the LEN is capable of handling four commercial access connections.

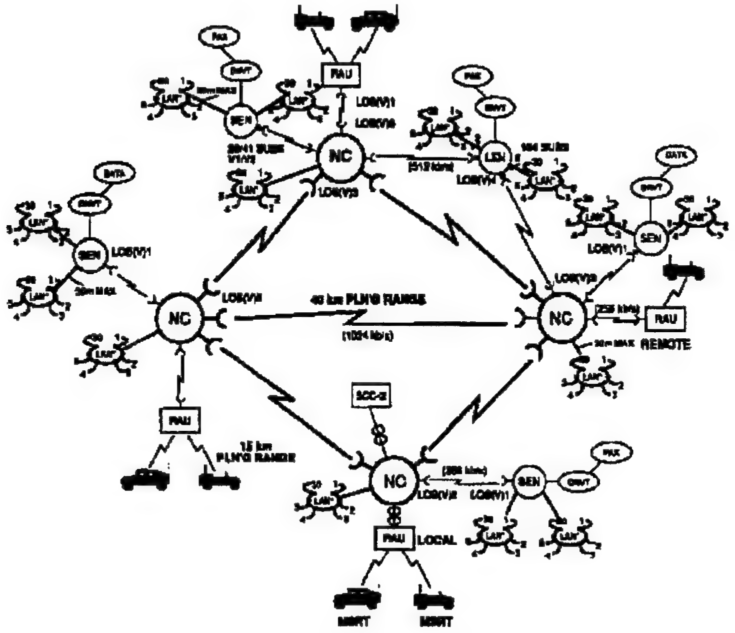
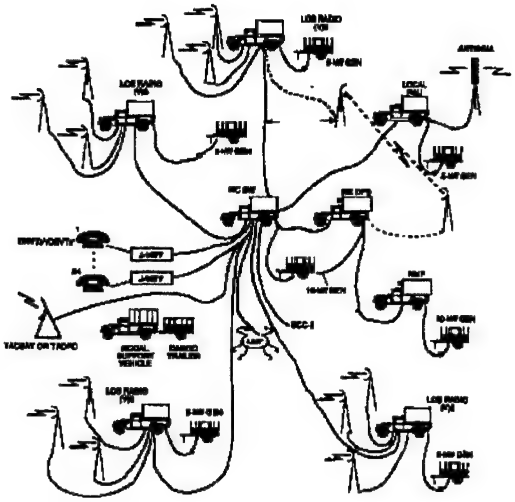
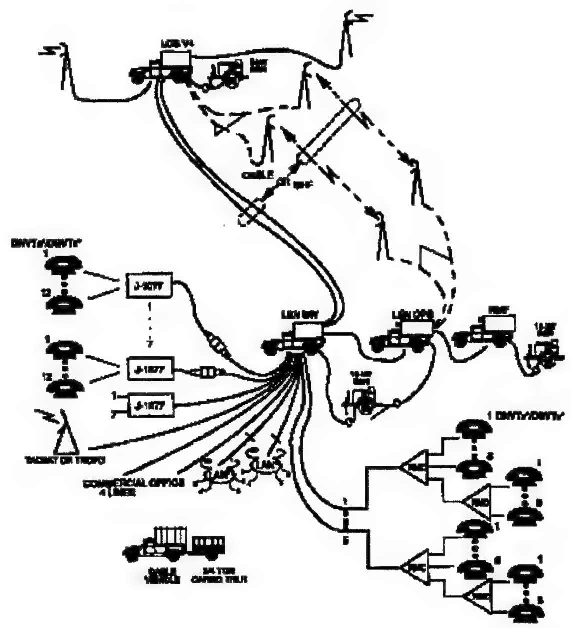


Figure 3. Division Network



- Supports 24 local subscribers
- Provides tactical packet network (TPN) connectivity
  - 2 ea - x.25
  - 29 ea - 802.3 local area network (LAN)
- Terminates up to 16 digital trunk groups
- Provides internodal connectivity to 5 (max) node centers

Figure 4. Node Center Switch (NCS)



- Supports 164 digital subscribers
  - 84 ea - 26 pair cable
  - 80 ea - remote multiplex combiner (RMC)
- Provides tactical packet network (TPN) connectivity
  - 7 ea - x.25
  - 116 ea - 802.3 local area network (LAN)
- Commercial access connections (4 ea)

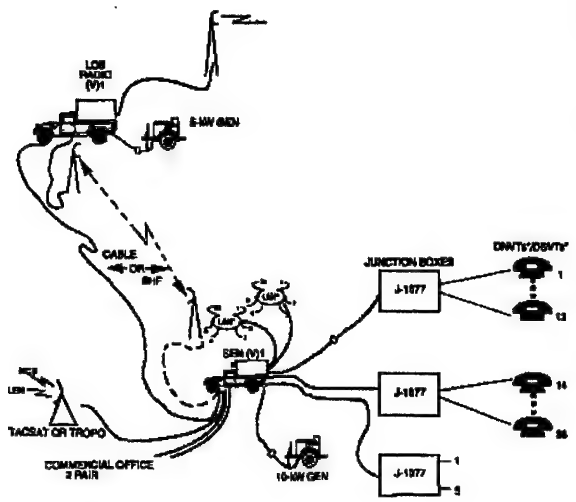
Figure 5. Large Extension Node (LEN)

8. Small Extension Node (SEN)

The SEN is available in two versions with different subscriber handling capacities. Version 1 can support 26 subscribers. Version 2 can support 41 subscribers. Figure 6 depicts the components of both versions. Each SEN version can provide TPN connectivity for X.25 connections, 802.3 LAN connections, and two commercial access connections. Additionally, the SEN provides a combat net radio interface (CNRI) that enables combat net radio operators to access the network.

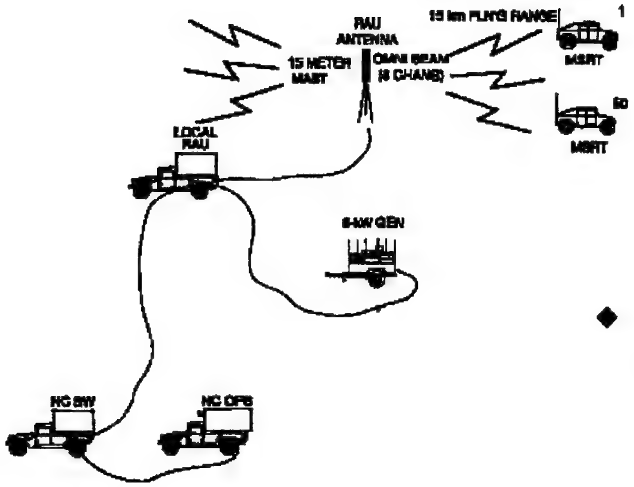
9. Radio Access Unit (RAU)

The RAU is the military equivalent of a commercial cell. It enables mobile subscribers to access the MSE network. The RAU is depicted in Figure 7. It provides omni-directional coverage for a 15 km radius and supports 25-50 subscribers. There are 92 RAUs in a notional corps and they are dispersed throughout the area of operation to provide maximum coverage for mobile subscriber access. As depicted in the division network, Figure 3, the RAU can be configured as a local RAU or a remote RAU. The local RAU is connected to the node center (NC) by cable. The remote RAU is connected to the NC by radio.



- Supports digital subscribers
  - SEN (V1) - 26 subscribers
  - SEN (V2) - 41 subscribers
- Provides tactical packet network (TPN) connectivity
  - 5 ea - x.25 connections
  - 58 ea - 802.3 local area network (LAN) connections
- Commercial access connections (2 ea)
- Provides combat net radio interface (CNRI) to the network via (KY-90)

Figure 6. Small Extension Node (SEN)



- Provides network connectivity to mobile subscribers
  - Omni-directional coverage
  - 15 km coverage radius
- Supports 25-50 subscribers

Figure 7. Radio Access Unit (RAU)

10. Subscriber Equipment

A major change resulting from the fielding of MSE is the subscriber equipment responsibility. The MSE subscriber equipment is user-owned and operated. The users must bring their own devices to access the system. The user-owned devices are called subscriber terminals. Section D listed the five types of subscriber terminals. The terminal types are the same at the EAC and ECB level. However, the models for the two levels can vary. The five types of MSE subscriber terminals are: 1) Digital Non-secure Voice Terminal (DNVT), 2) Digital Secure Voice Telephone (DSVT), 3) UGC-144 Communications Terminal (CT), 4) UXC 7 - tactical facsimile, and 5) Mobile Subscriber Radio Telephone (MSRT).

Figure 8 depicts the basic phone used for voice service. It is considered non-secure only because it contains no embedded communication security (COMSEC) capability. However, since the MSE communication system is secure, all calls within the network are secure. The DSVT (see Figure 9) is another phone instrument. It requires an embedded COMSEC key to operate it. Both the DNVT and DSVT operate at 16 Kbps and have data ports. The CT (see Figure 10) is used to pass data, and the UXC-7 is used to facsimile documents via MSE. Both terminals must connect to the data port of the DNVT or DSVT to transmit or receive information. The MSRT (see Figure 11) is a vehicle-mounted radio telephone that enables mobile subscribers to access the MSE network via RAUs. The user can call anywhere within the network as long as he is within communications range of a RAU.

F. CONCLUSION

This chapter provided information regarding U.S. Army combat communications at echelons corps and below. It culminated with information regarding the principal communication system for ECB, which is Mobile Subscriber Equipment. As a subset of the ATCCS, MSE facilitates the C2 process. MSE was designed to be a voice communication system. To further enhance C2, there must be voice communications and an efficient manner to pass data. The Tactical Packet Network takes advantage of packet switching technology to satisfy data requirements.

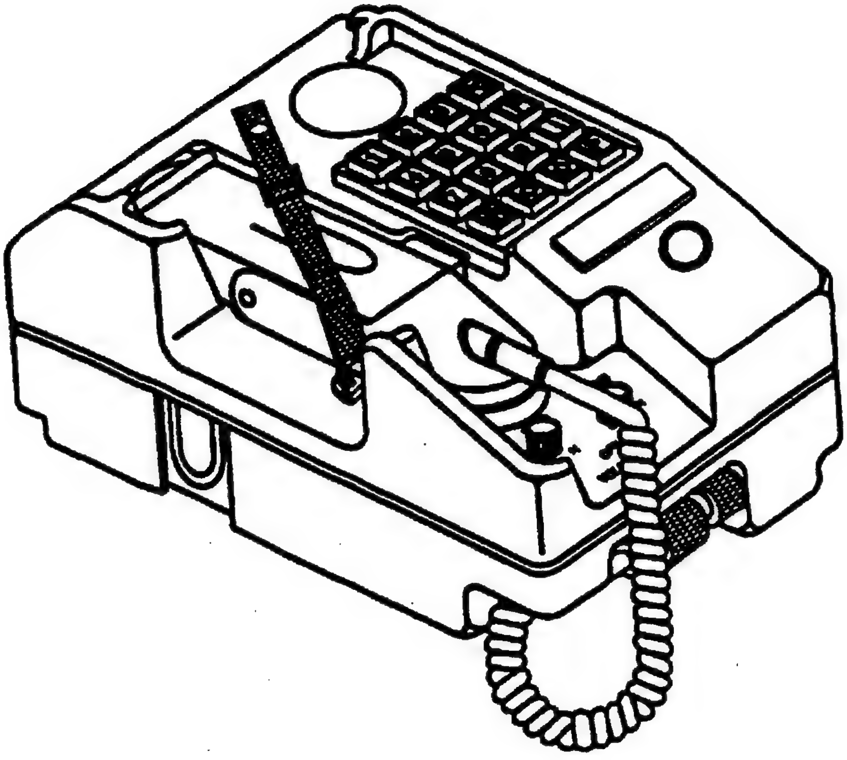


Figure 8. Digital Non-secure Voice Terminal (DNVT)

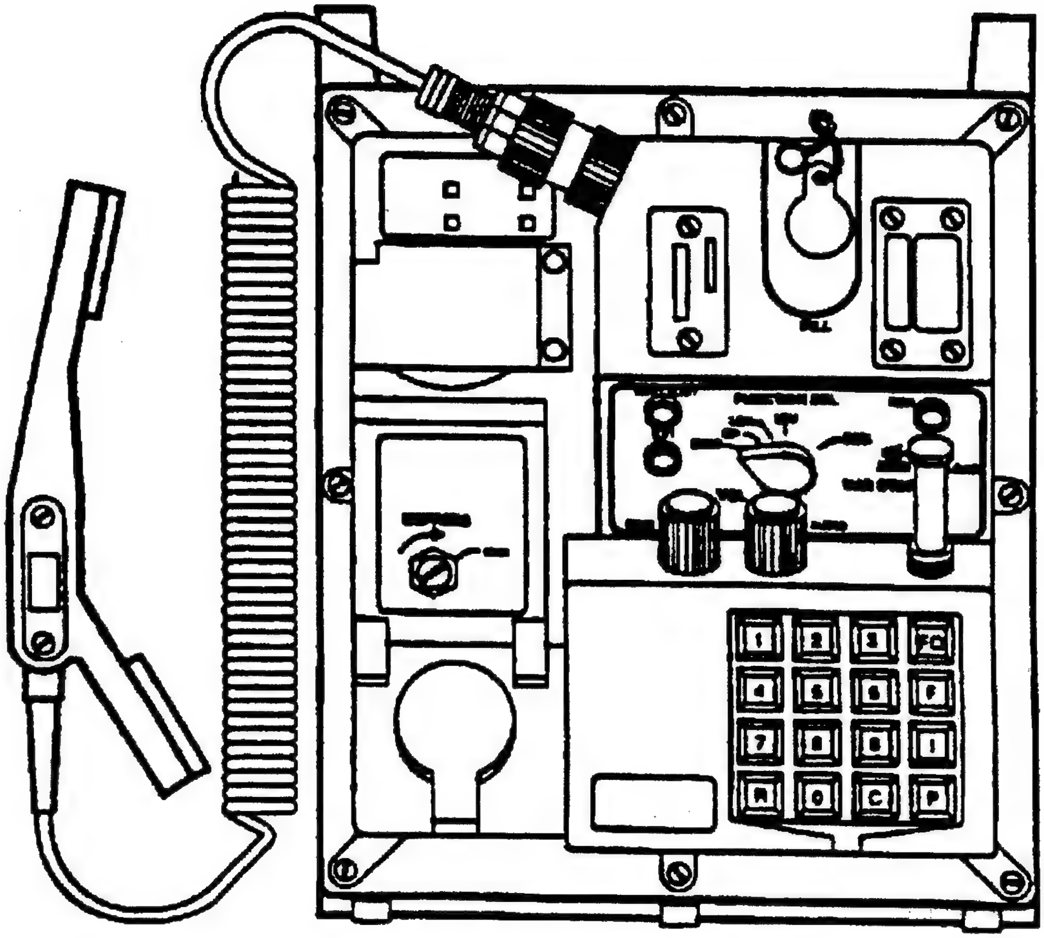


Figure 9. Secure Voice Telephone (DSVT)

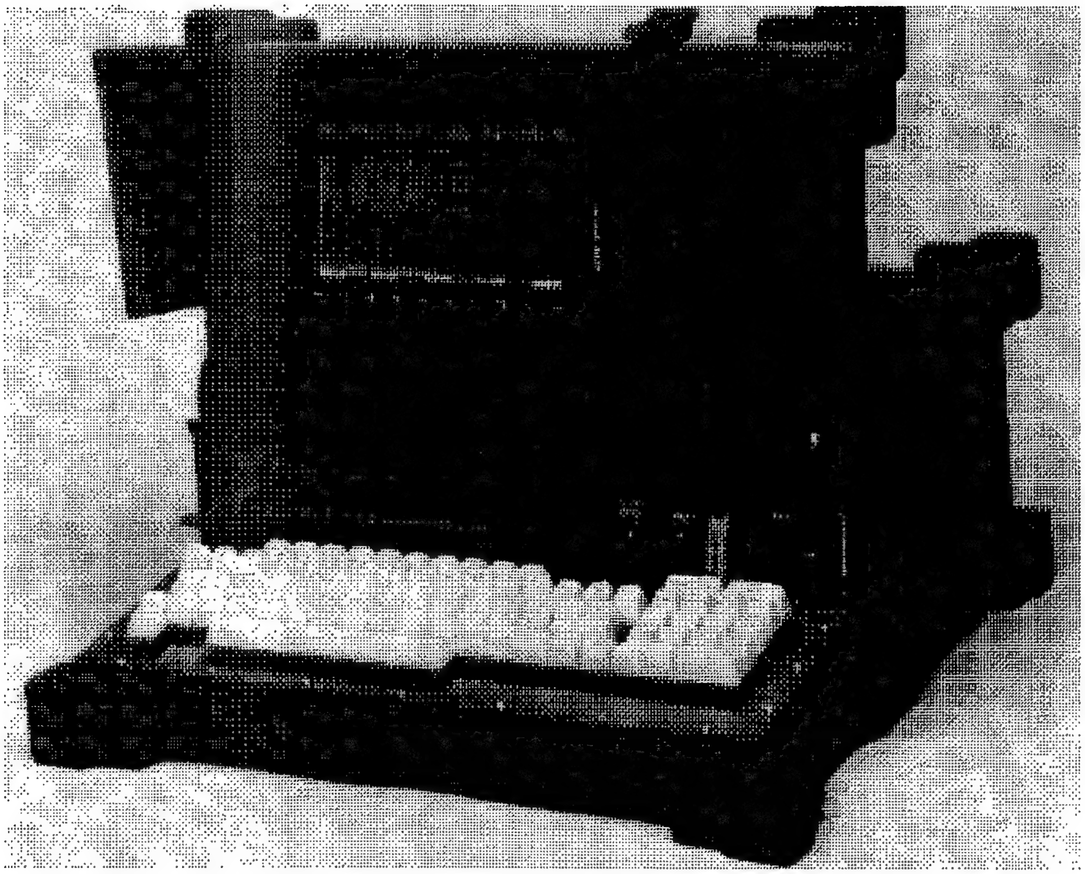


Figure 10. Communication Terminal (CT, AN/UGC-144)

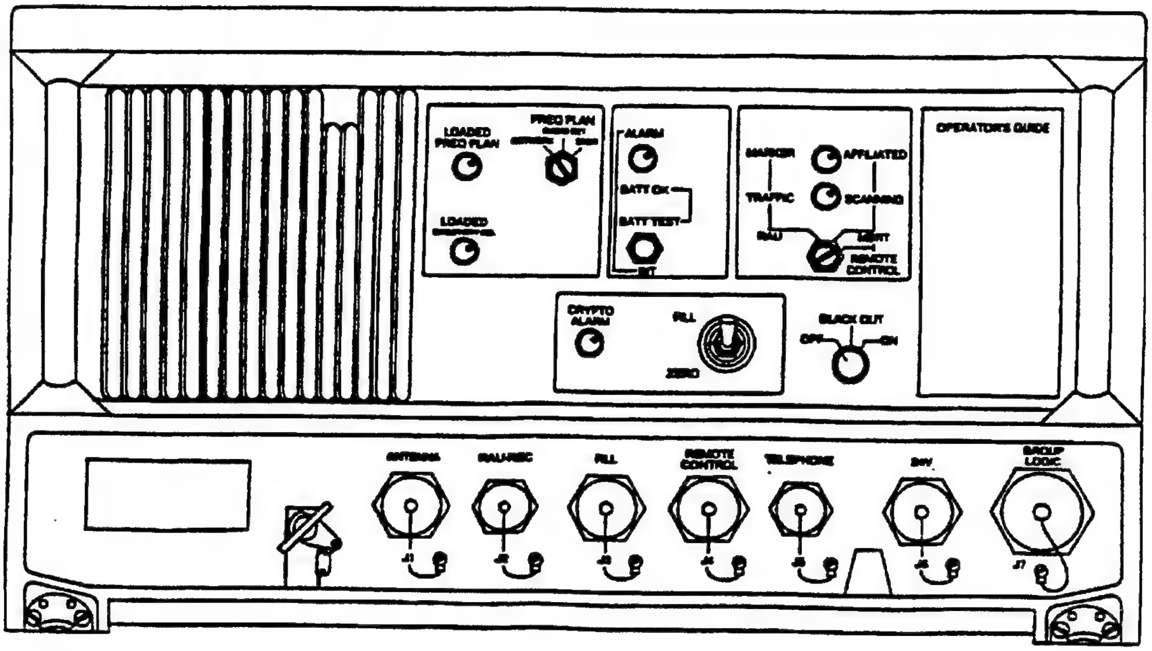


Figure 11. Mobile Subscribers Radio Telephone (MSRT)

III. PACKET SWITCHING CONCEPTS

A. INTRODUCTION

The goal of this chapter is to provide information regarding packet switching and to discuss some of the many issues associated with TPN. An overview of packet switching concepts is provided. Since it is this (packet switching) technology that is applied to TPN, this information should facilitate understanding TPN and related problems. The standards applied to packet switching are also relevant to TPN. Understanding packet switching concepts to include familiarization of the Open Systems Interconnection (OSI) model are stepping stones to knowing what the TPN involves.

B. PACKET SWITCHING

1. Types of Switching

a. Circuit Switching

There are two basic categories of switches, voice and data. The process of switching the signal can be accomplished in different methods. The most common manner is circuit switching [Ref. 6]. This is the type of switching that generally supports household phone requirements. The procedure involves the telephone company's central office establishing a connection between two stations with messages going directly from one telephone to another. Circuit switching dedicates a network resource to a call on an exclusive-use basis. As implied, circuit switching generally supports voice communications.

b. Message Switching

Message switching is the switching method used to support data requirements. In message switching, the entire transmitted message is accepted by the central switch and forwarded immediately, if possible, or stored and forwarded at a later time when circuits are free. Because of this procedure, message switching is often referred to as "store and forward" switching. The Department of Defense (DoD) automated digital network (AUTODIN) is an example of a message switch.

Message switching can use much narrower transmission bandwidths than voice communications. Therefore, accurate transmission is possible on poor-quality communications circuits. Old technologies that have now matured are being utilized to meet the growing information requirements. Packet switching is an example of old technology that's now at the forefront and being used by industry and the U.S. Army. As the information age continues to evolve, data and computer communications requirements have also evolved. New technologies are constantly being developed and implemented.

2. What is Packet Switching?

Packet switching, in large measure, is a special case of message switching, wherein the maximum message length is severely restricted [Ref. 7, p. 75]. It is a technique used to interconnect multiple remote computing environments. It divides the data into packets or groups of packets, then transmit them individually over the most efficient network paths. Normally, there are 128 characters per packet. Because it permits communications resources to be used at utmost efficiency, packet switching can adapt to a wide variety of user services and demands. Transferring information in packets can also result in increased efficiency and reduced costs to users of the network.

3. History of Packet Switching

Paul Baran and his associates at RAND Corporation in the early 1960s were credited with "inventing" packet switching [Ref. 7]. Packet switching origins were more strongly based in voice communications as opposed to data communications. Baran's ideas initiated with the idea of breaking a voice conversation between two parties into short separate pieces. These pieces were called packets. Figure 12 illustrates the concept.

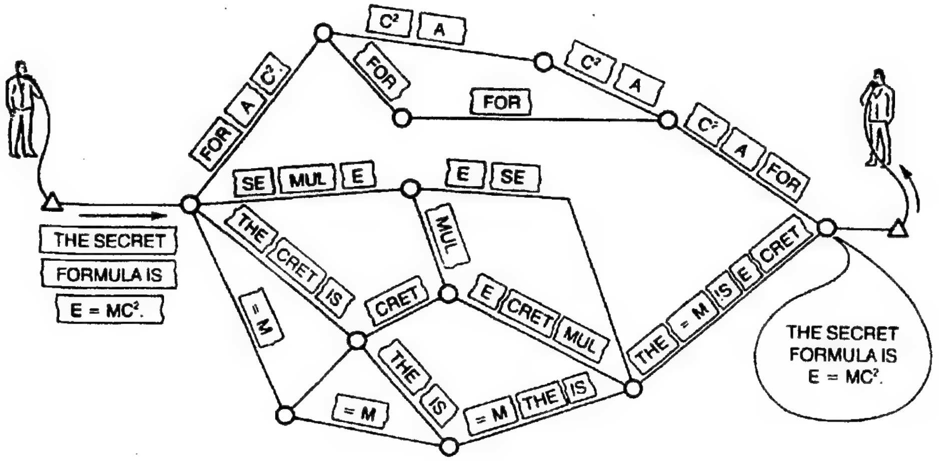


Figure 12. A Packet Switching Network used for Voice Communication
From [Ref. 7, p. 31]

The original message was parsed and sent over different paths. At the destination, the pieces were reassembled in the proper order to make the voice intelligible. From an operations security (OPSEC) standpoint, this was a great concept. Since bits of the message took different routes, the results of a wire tap or intercept would yield garbled information at best. These ideas have been around and published since 1964. But, the technology required to tackle the complex processing, routing, and control functions to implement this concept were not available.

4. Packet Switching Advantages and Disadvantages

a. Advantages

- Prompt Delivery of Messages: Packet switching offers several advantages as a means to transmit data. One advantage is the rapid exchange of short messages. Since the messages are broken down into packets, short messages could potentially fit into a single packet. A message contained within a single packet is unlikely to interfere with a long message divided among several packets. This provides efficiency and prompt delivery of short messages.

- Flexibility: Packet switching is flexible too. Since all the packets of a given message do not have to follow precisely the same route to the destination, the packet network is very flexible and adaptable. The benefit is that if a failure occurs during a particular transaction, the packet can be re-routed around the network.

- Speed of Conversions: Like message switching, the packet switching network can format, code, and speed conversions between unlike terminals. It appears non-blocking and can attain very high network efficiency as well as line utilization. These advantages are just a few of the positive impacts of packet switching technology.

b. Disadvantages

The principal disadvantage of packet switching is the manner in which it must be implemented to achieve its advantages [Ref. 7, p. 38]. Many small processors and switches must be employed to achieve the flexibility and adaptability required. The result is complex routing, control procedures requirements, and protocols to deal with network issues.

5. Packet Network Induced Errors

a. Packet Sequencing

One of the network issues inherent with packet switching is packet sequencing. As an example, three packets are sent out over the network in the sequence 1,2, and 3. But, due to network problems, i.e., retransmission of packet(s), they could arrive in a different sequence. To alleviate this problem, the packets must be reassembled at the distant end. Figure 13 is an example involving a sequencing problem. In this case, the packets are sent in order of 1, 2, and 3. Upon arrival at Switch 3, packet number 2 must be retransmitted due to an error. The result is that packet 3 arrives before packet 2 because it (packet 3) does not have to be retransmitted. At the destination the message is reassembled and placed in the original format or sequence.

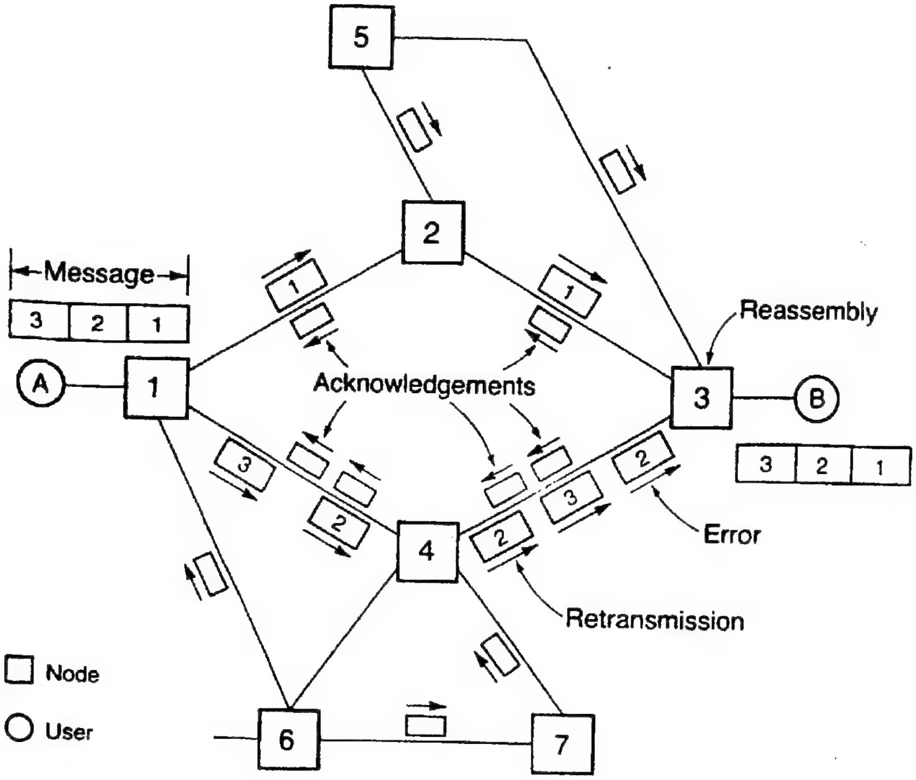


Figure 13. Basic Operation of a Packet Switched Network: Movement of Three-packet Message from User A to User B
From [Ref. 7, p. 77]

b. Acknowledgments

Acknowledgments are key to error checking in packet switching. Any information packet that is received is promptly acknowledged back to the sender. If the acknowledgment is not received by a certain time period, the sending switch assumes the packet contained errors and retransmits the packet. If the packet received contains minor errors a negative acknowledgment (NAK) is sent asking for a retransmission.

c. *Lost Packets*

Sometimes packets are lost. As an example, if a packet is sent to a switch and the switch acknowledges having received the packet, then the switch crashes. Figure 14 illustrates the loss of a packet. In this case, packet 1 goes to switch 2, switch 2 sends back an acknowledgment then fails before it forwards the packet. The result is that when the message is received, it does not contain all the packets. There are ways for the network to shield itself against lost packets. One method is to restrict switches from sending acknowledgments until the packet has been forwarded. Another manner is to require the sender to retransmit at the request of the receiver.

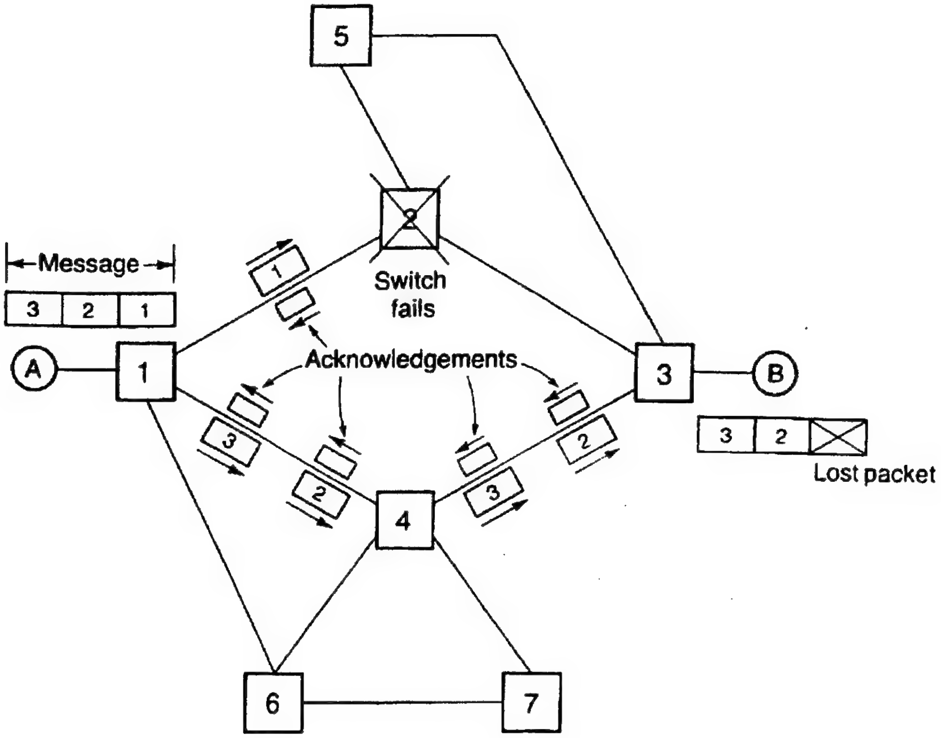


Figure 14. Basic Operation of a Packet Switched Network with a Switch Failure: Loss of a Packet

From [Ref. 7, p. 79]

d. Erroneous Duplication

In addition to being lost, packets can be erroneously duplicated. Figure 15 depicts a diagram illustrating how a packet can become duplicated. In this case, packet 1 goes to switch 2 and switch 2 sends the acknowledgment. However, before the acknowledgment is received the line fails. The originator never gets the acknowledgment and therefore assumes the message wasn't sent. So the message is resent. Since switch 2 also forwarded the message, there are two packet 1's at the destination.

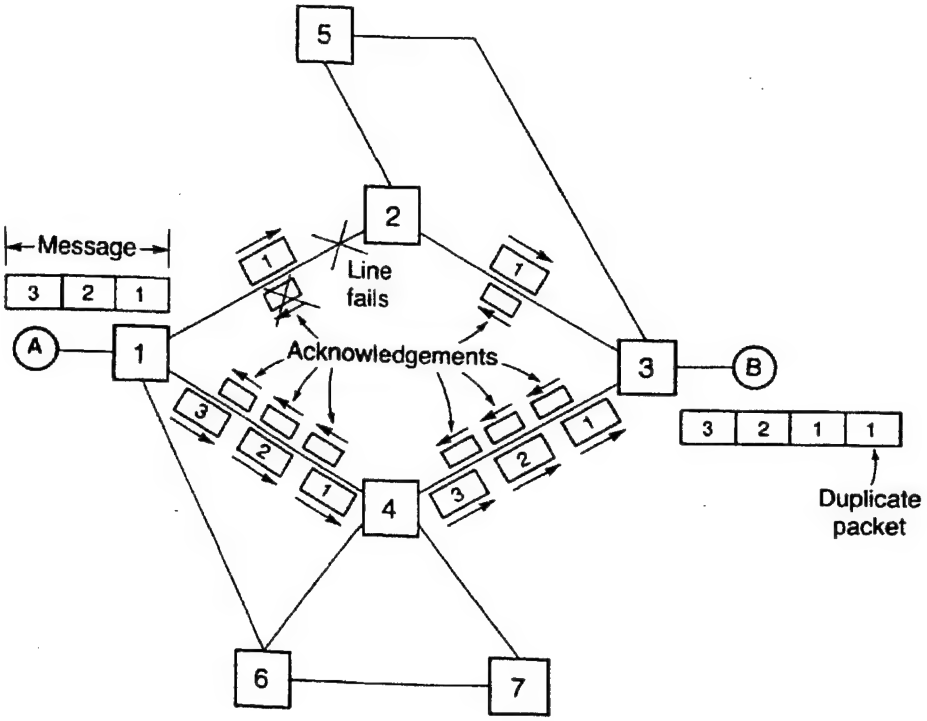


Figure 15. Basic Operation of a Packet Switched Network with a Line Failure: Duplication of a Packet
From [Ref. 7, p. 80]

6. Packet Switching Overhead

There must be some mechanisms in place to address the network-induced errors. The network contains a certain amount of redundant overhead information to protect against the errors mentioned. Overhead is information that has to be transmitted through a network in order for switches to properly handle the transmission and delivery of a call or message [Ref. 7, p. 81].

There are two formats for overhead. Overhead can be appended to each user packet or it can be in the form of self-contained acknowledgments or control packets flowing among the switches. In addition to overhead, there are well-defined rules and procedures known as protocols that must be adhered to while communicating.

C. OPEN SYSTEMS

1. Open Systems Interconnection (OSI)

By the 1970s, computer manufacturers throughout industry were developing data communication products. These manufacturers had foresight and recognized that the market would prosper during the 1980s and 1990s. Furthermore, they realized that future systems would be purchased based on their communication ability as well as processing power. Equally significant, manufacturers also recognized that communications would often involve systems from more than one supplier. Hence an open systems environment would be needed. Working with other manufacturers was viewed as not just a good idea but a necessity. In March 1977, at a meeting of the International Organization for Standardization (ISO) in Sydney Australia, it was proposed that a framework be laid down for communications between computer systems and other electronic equipment [Ref. 8].

Every country has its own standards body that establishes standards, e.g., American National Standards Institute (ANSI) and the British Standards Institution (BSI). The ISO is part of an international web of standards bodies. It is a body that is closely connected with industry and establishes standards for just about everything, including light bulbs. The committee members do not draw salaries from the ISO; they represent a multitude of firms and organizations and are paid by those organizations. The ANSI and BSI also have representation on the ISO.

It is the ISO that came up with the standards applied to most data communications equipment and systems in use today. The ISO produces documents that are passed through several stages so that the whole of ISO has an opportunity to provide comments or clarification. One such document is ISO 7498, the international standard for the basic OSI architecture. The OSI model has seven layers that serve as a blueprint for the communications structure between systems.

2. The OSI Seven-Layer Model

a. Introduction

The OSI seven-layer model serves as a guideline for the creation of open systems. It is a framework around which a series of protocols are defined. As the title indicates, the model contains seven layers. The purpose of the seven layers is to segment the various functions that must be carried out when two machines want to communicate [Ref. 6, p. 419]. The seven-layer OSI model is implemented via software that handles the transmission of a message from one terminal or application program to another distant terminal or application program.

b. Physical Layer

The first layer (bottom) of the OSI seven-layer model is the physical layer. It is the lowest layer and is primarily concerned with transmitting data bits across the medium. At this layer, hardware is the concern. Examples include: cables, signal drivers, transformers, and parallel to serial converters. Layer 1 is the basic link through which all data must pass.

c. Data Link Layer

The second layer is the Data Link Layer. This layer manages the basic transmission link established in layer 1. It controls the flow of data, the correction and detection of errors, and sequencing. It is at this layer that acknowledgments are sent back to acknowledge that data was received. Additionally, the data link layer establishes and controls the path of communications before sending the message down to the physical layer below it. The X.25 protocol that the TPN uses is a data link protocol.

d. Network Layer

The network layer is the third layer of the OSI seven-layer model. This layer controls routing and other functions such as flow control and sequencing. The network layer provides the services needed to move data through the network to its destination. When you make a phone call, the telephone network carries out the functions of the network layer. Although transparent to the user, the telephone network determines the most expeditious routes for routing for the call.

e. The Transport Layer

Layer 4 is the transport layer and is often called the host-to-host layer or end-to-end layer because it establishes, maintains, and terminates logical connections for data transfer between end users. This layer deals with issues such as addressing as well as procedures for entering and departing from the network. Additionally, the transport layer prevents one host from overrunning another host by controlling the movement of messages.

f. The Session Layer

The fifth layer of the OSI seven-layer model is the session layer. The session layer is responsible for establishing the connection between two applications and re-establishing the connection if it fails. It is referred to as the data flow control layer because it arranges the way data should be sent, i.e., in both directions at once, in alternate directions, or in one direction. Peter Judge, author of *Open Systems*, explains the session layer as being like the rules of conversation. For example if you call someone, you identify yourself and agree how the conversation will go. One person talks or both.

g. The Presentation Layer

Layer 6 is the presentation layer. This layer determines how data is represented. It performs the necessary transformations and formatting to present data to end users. The key idea is to ensure both computers are using the same language resulting in a common representation for the end users.

h. The Application Layer

The last layer (top layer) of the OSI seven-layer model is the application layer. The application layer does not contain application programs. It provides a set of utilities for application programs. This is the end user's access to the network. This layer is where application programs, terminals, and computers access the communications network.

D. CONCLUSION

This chapter provided background information regarding the concepts and operations of packet switching. The advantages of packet switching clearly outweigh the disadvantages. Although there is a price to pay in terms of overhead to resolve network induced errors, the efficiency of packet switching makes it worthwhile. The fact that it operates in an Open Systems environment is an additional benefit.

IV. THE TACTICAL PACKET NETWORK

A. INTRODUCTION

Chapter III discussed packet switching concepts in general. Those concepts are key to understanding the Tactical Packet Network (TPN). The aim of this chapter is to build upon that knowledge and explain the U.S. Army's Tactical Packet Network. Key aspects of TPN include network configuration, TPN equipment, packet-switching and routing, TPN protocols, TPN messaging and Tactical Name Servers. The TPN issues are relevant to the system's performance.

B. THE TPN STRUCTURE

1. What is TPN?

The TPN is a combination of the MSE Packet Network and the EAC Packet Network. It is a packet switching network for tactical users that is based on industry packet switching standards. For example, it uses X.25 and 802.3 protocols, as well as TCP/IP. The TPN is layered over the MSE-Circuit Switched Network with Packet Switch (PS) equipment co-located with the circuit switch equipment. Circuit switch trunks within a MSE digital trunk group (DTG) are specifically reserved for TPN usage.

2. Simple TPN Deployment

The TPN deployment can range from simple to complex. Typically, a simple deployment, as reflected in Figure 16, can be a simple MSE Packet Network (MPN). In this figure, each node has packet switching capabilities. The key difference is the type of switches and the throughput for the Node Center Switch (NCS) and Small Extension Node (SEN). Both the equipment and throughput will be discussed in subsequent sections.

3. Complex TPN Deployment

Figure 17 is a more complex network that really demonstrates the power of TPN. Because of the commonality of equipment and protocols, data can traverse several different types of networks. Although this figure is a simple representation of a complex system, the MPN architecture can be complex.

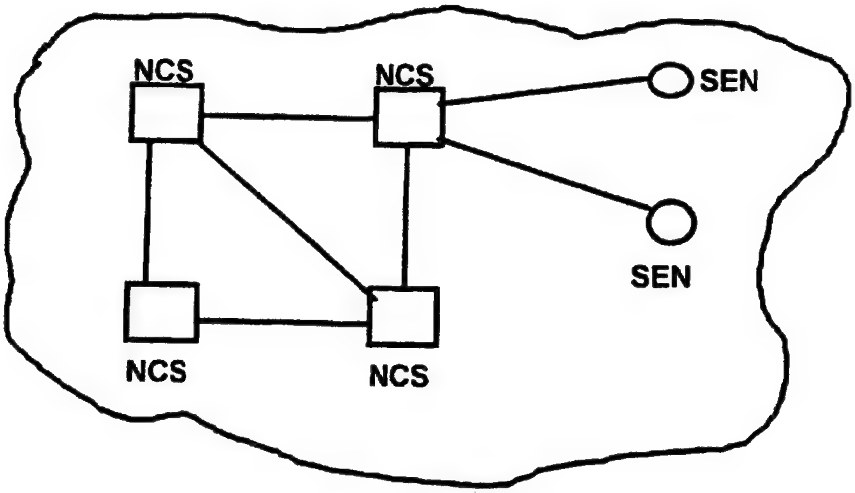


Figure 16. Single MSE Packet Switch Network
From [Ref. 9, p. 2]

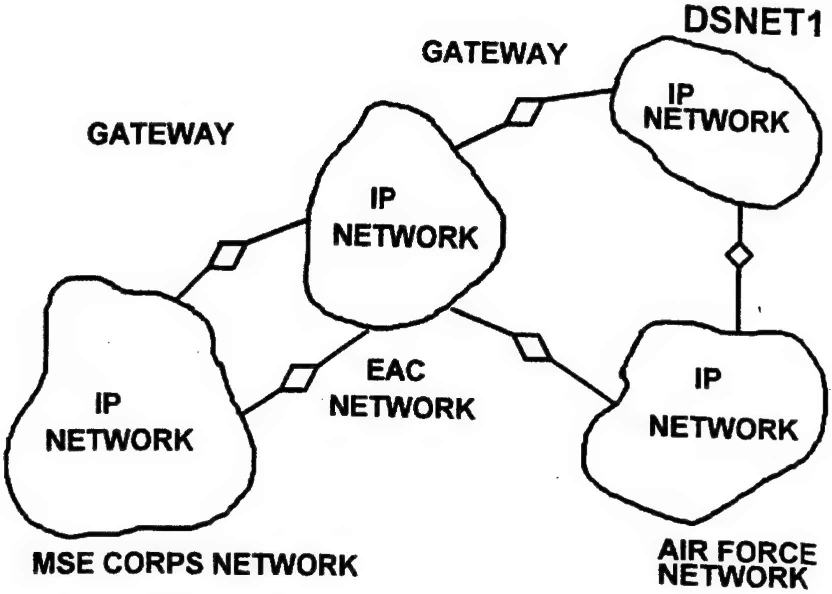


Figure 17. Internetwork of Networks
From [Ref. 9, p. 3]

4. MSE Packet Network Deployment

The MPN is used at Echelons Corps and Below (ECB). The ECP system depicted in Figure 18 shows packet switching connectivity for the MPN. There are different capabilities, i.e., 802.3 (LAN) users and X.25 subscribers, dependent upon connectivity to the Node Center, the Large Extension Node, and the Small Extension Node.

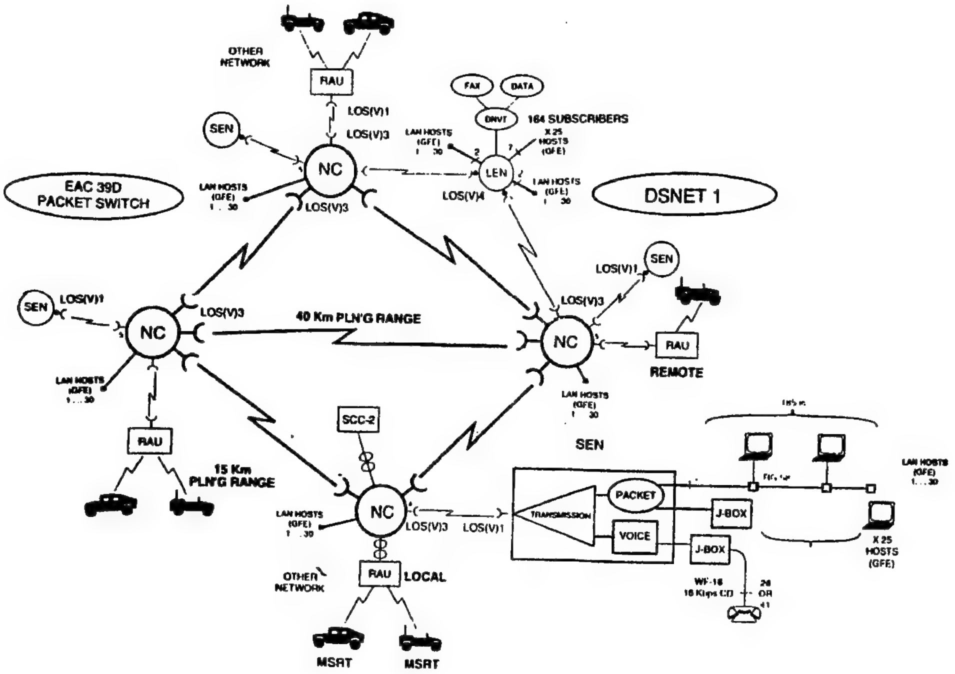


Figure 18. ECB Communication System
From [Ref. 13]

5. TPN Equipment

The TPN equipment consists of two types of packet switches and two workstation versions. This section addresses the packet switches. However, some of the functionalities provided via the workstation, i.e., Message Transfer Agent (MTA) and Tactical Name Server (TNS) will be discussed later.

The two types of TPN switches are the AN/TYC-20 and the AN/TYC-19. The key difference is that the AN/TYC-19 is a gateway switch. The gateway switch enables packets of information to traverse external networks, i.e., EAC networks and the Defense Data Network (DDN). The AN/TYC-19 is always positioned at a node center. The AN/TYC-20 is positioned at the SENs and LENs. It operates as an X.25 concentrator and transport switch, compatible with X.25 and X.75 standards. It also provides two Ethernet ports and 11 ports for X.25 subscribers.

C. PACKET SWITCHING AND ROUTING

As Chapter III explained, in packet switching, the message is broken down into packets called datagrams that can take different routes. The TPN uses a Shortest Path Routing algorithm that conducts a real-time analysis of network delay before routing X.25 packets through the network on a packet-by-packet basis. Before a packet is forwarded, a routing table designates the next path to which the packet is forwarded. This routing table further indicates whether or not the destination packet switch can be reached. To remain current, the routing process continuously updates the routing table based upon information gathered by itself and every other packet switch.

The AN/TYC-20 gateway switch performs IP routing between TPN network boundaries and external networks. The protocols used for IP network boundaries and external networks are different. The Interior Gateway Protocol (IGP) is used for internal actions and currently the Exterior Gateway Protocol (EGP) is used for external routing. The EGP will be replaced by Border Gateway Protocol (BGP) in 1997. Both protocol types will be explained in Chapter V.

D. TPN PROTOCOLS

1. The DoD Protocol Layers

The TPN protocols are key to the multitude of benefits gained by using industry standards. Figure 19 depicts the DoD protocol layers and the services provided at the various layers. In this case, there are five of the seven OSI layers depicted. The Implementation Layer and the Presentation Layer are omitted. Also, there are other proprietary protocols used in TPN that are not shown. The Ethernet and LAN standards correspond with the data link and physical link. The 802.3 and X.25 protocols mentioned earlier are Ethernet and LAN standards. Subsequent sections provide the features afforded via the other layers.

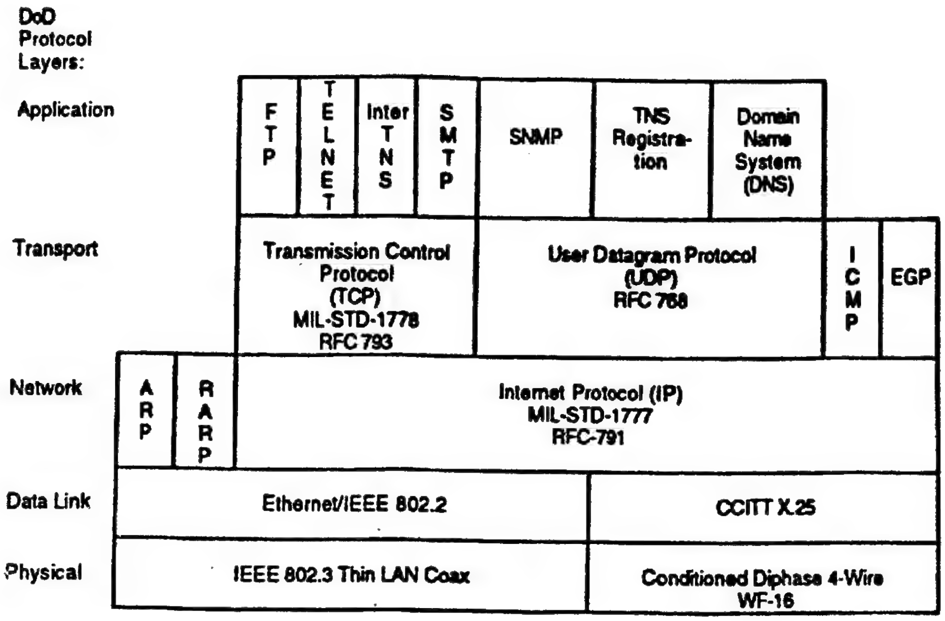


Figure 19. Some Protocols Used Within TPN
From [Ref. 10, p. 11]

2. Application Layer

The Application Layer offers a multitude of services to the user. The first is file transfer protocol, commonly referred to as FTP. FTP is a file manipulation process that allows users to move files back and forth. Telnet is another file manipulation utility. The tool that allows users to locate each other is called the Tactical Name Server (TNS). The TNS also contains a registration capability which is used to register hosts. Domain names occur via the Domain Name System. The protocols for email and network management are: Simple Mail Transfer Protocol and Simple Network Management Protocol, respectively.

3. Transmission Control Protocol/Internet Protocol (TCP/IP)

a. What is TCP/IP?

Transmission Control Protocol is the protocol frequently mentioned in conjunction with Internet Protocol. As Figure 19 reflects, TCP is associated with the Transport Layer and IP is associated with the Network Layer. Several of the protocols that comprise the Network and Transport Layers were designed for TCP/IP communication.

TCP/IP was developed as a U.S. military standard for interconnecting internets among different Local Area Network environments. It allows reasonably efficient and error-free transmission between different systems. TCP is based on the Datagram Model of network routing which is easier to implement than the alternative virtual circuit model [Ref. 11, Chapter J]. Because it is a file transfer protocol, it can send large files of information across sometimes unreliable networks with great assurance that the data will arrive in an uncorrupted form [Ref. 6].

b. TCP/IP Operations

When TCP/IP is used, data travels between sender and receiver applications inside segments created by TCP models. The information to be transmitted is broken down into pieces that travel inside packages of a special format called IP datagrams. The IP datagrams allow the TCP segments to take different routes through the network as packets in a packet switching network. The segments are able to travel by different data streams. On the receiving side, a TCP software package collects the IP datagrams, extracts the data, and puts it in the proper format. If some datagrams are missing, the receiver asks the sender to retransmit them.

c. TCP/IP Simplified

Jerry Fitzgerald, author of *Business Data Communications* provides a simple explanation of TCP/IP. To understand TCP/IP, imagine the data being sent across the network as a document. This document has many typed pages. In fact, there are so many pages that they must be separated into several stacks and placed in a series of separate interoffice envelopes. Each envelope is identified by a sequence number so the recipient knows the correct order in which to read the pages. Each of these interoffice envelopes is then inserted into a large mailing envelope with the destination office address added for mailing purposes. The typed pages represent application data, the interoffice envelopes represent TCP segments, and the large mailing envelope represents the IP datagrams.

4. Transport Layer

The transport layer consists of the TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) and EGP. As implied in the previous section, TCP allows a process on one machine to send a stream of data to a process on another. The UDP uses IP to deliver datagrams. The principal difference between UDP and IP datagrams is that UDP includes a protocol port number that allows the sender to distinguish among multiple destinations (application programs) on the remote program. If there is a problem with the datagram, the ICMP sends reports of the problems back to the original source. The EGP is used to advertise the IP addresses of networks so that they can be reached in the autonomous system.

5. Network Layer

The Network Layer is comprised of Address Routing Protocol (ARP), Reverse Address Routing Protocol (RARP), and Internet Protocol (IP). As previously discussed, IP is used in conjunction with TCP. It defines the IP datagram as the unit of information passed across the internet. The ARP, allows a host to find the physical address of a target host on the same physical network, given only the target's IP address [Ref. 12]. The RARP, on the other hand, is used by diskless machines to find their IP address.

E. MESSAGING WITH TPN AND THE TPN MTA

1. Node Center Switch Message Transfer Agent

A TPN-connected host uses the Node Center Switch Message Transfer Agent (NCS MTA) to send an electronic mail message to another user or list of users in the TPN. Although the NCS MTA uses the SMTP over TCP/IP, the host must have its own SMTP compatible mail agent and user agent (UA). The UA is located at the host. Its purpose is to generate and display email. However, it does not deliver or accept messages. Instead, it uses the mail agent within the host to perform these functions by sending the mail directly to another mail agent or via the NCS MTA.

2. Sendmail

Sendmail is the software package that provides the NCS MTA message routing capability. It is a SNMP-based mail routing system that relays incoming and outgoing mail to the appropriate recipient or a list of recipients for delivery. Although sendmail can be configured in various ways for TPN, the configuration file is fixed and can be dynamically modified in the field. For NCS MTA, the configuration results in the following major services [Ref. 10, p.15]:

- An SMTP server for receiving network mail transfer
- System-wide mailing list
- Message queuing for re-attempting failed deliveries
- Delivery of error messages to senders of unsuccessful mail delivery
- Access to the TNS for name resolution.

F. THE TPN TACTICAL NAME SERVER (TNS)

1. What is TNS?

The TNS is a dynamic database that is made up of hosts and mailboxes whose main activity is to answer queries form hosts and from the MTA. The database is dynamic because a host or a mailbox can relocate anywhere within the TPN. When a host relocates, the local TNS receives the new registration information and passes it on to the other Tactical Name Servers.

2. The TNS Domain

The TNS network may consist of one or more IP networks called a TNS domain. The TNS Domain is needed because one network can not contain all the necessary packet switches. The software used in TNS domain is Berkeley Internet Domain (BIND) server software that is based upon the Domain Name Server Internet Standards. Generally, the boundary of the TNS domain is the boundary of the Corps.

3. TNS Functions

The TNS has three main functions. The first function is to support host registration and store names to IP address bindings. The second function is to synchronize and manage TNS databases: Network User Database, Local User Database, and Domain Database. The third function is to respond to queries from the hosts and from the NCS MTA.

4. TNS Databases

a. Network User Database

The three TNS databases are associated with functionality. The TNS Network User Database contains hosts and mailboxes that are presently registered in the TNS network. It is also used by the name server to answer queries or to search for duplicate IP addresses or names during the registration process. The TPN Network User database is automatically updated on a periodic basis with new host registration information and mailboxes.

b. Local User Database

The TNS Local User Database contains all hosts and mailboxes registered at the local TNS. It is used by the local TNS to manage the registered hosts and mailboxes associated with it. However, the Local User Database can not be modified by the operator directly.

c. Domain Database

The Domain Database is the only database that can be modified by the operator directly. It consists of domain names, Net ID assignments, Packet Switch numbers of potential TNS neighbors, and pointers to other domains. The IP addresses of other domain name entries are also maintained in the Domain Database.

G. CONCLUSION

The Tactical Packet Network represents the U.S. Army's data communication capability. It involves a myriad of operations to get the message through. The TPN problems normally occur because some of the functionalities aren't performing as specified. Therefore, it is important to understand the total TPN system.

V. TACTICAL PACKET NETWORK ISSUES

A. INTRODUCTION

The TPN already has progressed from a planned acquisition to a fully-fielded system. While TPN fills a previous void in terms of data processing, there are still challenges associated with TPN. There were a multitude of issues that surfaced during the fielding, some of which were resolved on the spot. Some of the problems have near-term solutions that are just that, near-term. There are scheduled changes designed to increase the throughput and workaround resolutions aimed for most of the TPN problems. This chapter discusses some of the issues using a categorized format. The categories are: software, interoperability, throughput, security, and gateway protocols.

B. SOFTWARE

1. Internodal Trunk Markings

One of the software problems associated with TPN during fielding was the disastrous effects of incorrectly marking packet switch inter-switch trunks (ISTs) across IP boundaries. For example, if two node centers wrongly marked an internodal as "packet = yes", when the link should have been marked "packet = no", or "packet = gateway", the Packet Switch Network would go ahead and install the packet trunk [Ref. 13]. This problem was difficult to fix for the Wide Area Network (WAN) manager and the Network Management Center (NMC). The recommended solution was to have the PSNs shut down and submit a trap. A trap is a message triggered by network components experiencing problems [Ref. 14, p. 10]. The software would be able to detect if the Packet Switch Nodes (PSNs) assigned to different IP networks detect a trunk when it should be a gateway link. Concurrently, the Nodal Management Center (NMC) would be notified, enabling the WAN manager to proactively fix the problem.

2. Duplicate PSNs

Another software challenge encountered during the fielding was the situation whereby two Packet Switch Networks in the same network had the same Packet Switch Number. If a PSN was just entering the net and detected a duplicate PSN number in the same network, it would reboot. This rebooting impacted negatively upon building the network. The proposed solution was to have the software detect a duplicated PSN in its own network and generate a trap report to the NMC. Additionally, the PSN light emitting diodes could flash to alert the operator. Subsequently, the software was modified to query the TNS database of all active TNSs and provide output in a tabular format.

3. Exchange Processes Dying

Problems within the TNS occurred during a V Corps Ironsides Victory Exercise. Specifically, TNS exchange processes died, posing several problems for the operator. The message "TNS not running" frequently appeared on the Input Systems Parameters screen at the Node Center. Sometimes the message "MTA not running" also appeared [Ref. 15]. The impacting results were, although the operator could do a host name query, the operator could not manually register any hosts. Additionally, if the operator cycled through the "Input Systems Parameters" whenever the message "MTA not running" appeared, the workstation would freeze, requiring rebooting the workstation online program.

4. TNS Registration Utility

During the Atlantic Resolve 94 (AR 94) Training Exercise, the 22nd Signal Brigade tested new TNS software from the Communications Electronic Command (CECOM) Software Engineering Division (SED). The program was a TNS registration utility that worked quite well, but caused confusion among mail users. The software gave users the option to register mailboxes, which was unnecessary except for Mobile Mail Recipients (MMRs). The recommended solution was to have this feature as an advanced option.

5. Node Switch Lookup (NSLookup)

Another TNS software utility tested during AR 94 was the NSLOOKUP program. The NSLOOKUP program had difficulty obtaining domain database downloads.

Nevertheless, the Network Operating System (NOS) program worked. The NSLOOKUP was not a grave concern due to the limited number of Windows-based hosts. However, as the number of users increase, the problem becomes more immense.

6. Registration Processes Dying

The third software utility tested during AR 94 was NPT Software Version 1.1.1. This version included TNS registration capabilities. The problem was that the registration processes died at random intervals. As a result, the operator had to restart the registration process by rebooting the system.

C. INTEROPERABILITY

1. TPN versus DMS Protocols

As was annotated in Chapter IV, the TPN switches are the same at the EAC and ECB levels. The gateway switch (AN/TYC-19) provides interconnectivity for different levels. However, from a futuristic standpoint, there can be interoperability problems when the U.S. Army implements the Warrior Information Network requiring TPN connectivity to the Defense Message System (DMS).

The two systems, DMS and TPN use different protocols. The DMS is an X.400/X.500 based messaging and directory system that will replace the Automated Digital Network (AUTODIN) system and individual email messaging systems. X.400 is the Consultative Committee for International Telephony and Telegraphy (CCITT) protocol for electronic mail. It defines how a worldwide mail system operates [Ref. 6]. X.500 defines how to develop a worldwide directory for user names and email addresses. X.400 provides greater functionality than that provided by SMTP. Additionally, while the naming service capabilities of X.500 are conceptually the same as TNS, the scope of X.500 directory services is much greater than that of the TNS.

The X.400 and X.500 standard meet today's functional needs and are tailored for growth to suit tomorrow's requirements. However, the development of products for the two is disproportionate. While the X.400 products have matured, X.500 products have not reached maturity. Nevertheless, X.400 and X.500 products are flexible enough to be configured for TPN use off the shelf.

The off-the-shelf solution could resolve the interoperability problem. The TPN would have to be upgraded to support X.400/X.500. But, there are some tradeoffs. First, the X.400/X.500 upgrade will result in increased overhead on the backbone (node centers). Although the increase is expected to range between 15-20 percent, other factors such as MTA distribution, Directory System Agent (DSA) distribution, and mail routing schemes could increase the percentage.

Increasing the backbone data ratio from 64 kilobits per second (kbps) to 192 kbps would make the TPN upgrade feasible. But, there is another issue. The additional overhead associated with the Directory Access Protocol (DAP) will require 200-250 percent more bandwidth that that currently used by TNS registration and query messages.

The current assumption is that the DSA will be located at backbone nodes. The potential problem with this is that it could cause problems on exterior links that support larger user communities, such as the Large Extension Node (LEN). The solution is to use a Connectionless Lightweight Directory Access Protocol (CLDAP) in lieu of DAP. Unlike DAP, in CLDAP, user interactions with the directory will not result in an increase in traffic. The CLDAP protocol is relatively new with less overhead requirements. It is expected to reach maturity in 1997.

2. Interoperability Solutions

a. The Three Choices

Reference 10 list three alternatives to resolve the TPN/DMS interoperability issue. The first option is to provide something that can be configured for usage. The second alternative is to provide an X.400/X.500 gateway within TPN. The third option is to upgrade TPN to X.400/X.500.

b. Configurable Item Option

The aim of option one is to provide a configurable item with the current Mail Transfer Agent (MTA) to allow mail to be routed to the Multi-Function Gateway (MFG). The MFG is being developed as a product to support several message domains, including X.400 and SMTP. While the MFG will support the exchange of messages from TPN to DMS and vice-versa, no gateway services are provided. Mail interoperability is provided, but directory interoperability is not.

The advantage of the MFG is that it requires minimal TPN changes. There are however, several disadvantages to this MFG option. First, it only provides mail services; users will not benefit from the X.400/X.500 features. Secondly, growth potential for TPN services will be limited. Additionally, conversions restrictions will apply and users must rely on an additional component which is not under TPN control (the MFG) for all messaging interactions with DMS.

c. Application Level Gateway

The second interoperability option provides an application level gateway that requires no changes to the current TPN architecture. The application level gateway would allow conversions of SMTP messages to X.400 before being forwarded to DMS. One advantage of this method is that the user software and TPN-to-user interface remains unchanged. Another benefit is, a TPN gateway could be used to send messages into other networks in addition to DMS.

The disadvantages of the application level gateway solutions are similar to those of the MFG option. Users will not be able to take advantage of the additional X.400/X.500 features, growth potential for TPN services will be limited and conversions restrictions will apply.

d. Upgrade to X.400/X.500

The third option and the recommended solution of Reference 10 will provide an upgrade to X.400/X.500 within TPN. There are several advantages for upgrading. First, the message transfer agent in TPN will be replaced by X.400 MTA and the Tactical Name Server will be replaced by X.500 Directory System Agent. Secondly, an X.400 SMTP application gateway will be included. Thus, SMTP users will continue to be supported until they transition to an X.400 user agent. Another advantage is that users will benefit from many additional X.400 and X.500 services. Lastly, TPN will have the greatest growth capabilities for providing services and it can eventually become part of the global directory.

As with the previous options, there are disadvantages associated with the upgrade solution. There will be: 1) additional overhead traffic, 2) additional storage requirements for the Directory Information Base (DIB), and 3) message stores and MTAs/DSAs will have to be procured or developed and configured for TPN needs.

D. THROUGHPUT

1. Units Report Bandwidth Problems

One of the biggest challenges with TPN is the throughput. The U.S. Army Signal Center Directorate of Combat Development (DCD) hosted a Tactical Automation Conference in 1994. The TPN bandwidth was among the key topics discussed. Several units indicated that they were having TPN bandwidth problems. Also, several after action reports (AARs) of training exercises reveal that the SEN bandwidth provided just isn't enough. This section looks at some of the problems encountered, the solutions, and the gateway protocols (EGP and BGP).

2. LAN Applications Impact Wide Area Network

As the previous section implied, the NC throughput will have to be increased to meet future DMS interoperability requirements. For now, units continue to do workarounds or quick fixes. Part of the problem is that many units were attempting to use applications designed to run over LANs in a WAN (TPN) environment. Typically, LANs have more available bandwidth than WANs. Also, client-server applications may be written either as LAN or WAN applications or both. Two possible solutions are use the existing bandwidth efficiently and optimize the environment the application was written for.

3. Documents Impact Bandwidth

During an exercise conducted at Fort Hood, the transmission of Powerpoint slides resulted in the need to time-share the TPN. Powerpoint slides and graphical slide formats generally contain unit insignia, unit logos, and other non-standard symbols that have significant impacts on the SEN and LEN bandwidths. Even word processor documents, such as those produced in Microsoft (MS) Word, have impacts because of their size in comparison to an American Standard Code for Information Interchange (ASCII) file. The MS Word document is ten times larger than ASCII.

4. Network Operations Affect Throughput

Other bandwidth absorbers are the TNS queries and pings. A ping is a TCP/IP program to test the reachability of destinations by sending an ICMP echo request and waiting for a reply.

5. Quickfix Bandwidth Solutions

There are a multitude of quick-fix solutions to some of the problems mentioned in the previous section. The first set of solutions involve stopping whatever action is causing the problem. For example, users can stop sending Powerpoint slides, MS Word files, and complex graphics. Instead, they can use common symbols, avoid logos, and send ASCII files. Additionally TNS queries and pings can be done less frequently. Another less attractive alternative is to have Command Posts prioritize TPN backbone access. All the above are easier said than done.

6. Information Management Schedule Imposed

The 2nd Armored Division implemented an Information Management Schedule during one of its exercises. The plan accomplished three things. The first thing is that it prioritized and established 15 minute time slots on an hourly basis. The All-Source Analysis System transmitted during the first 15 minutes (00-15). The Tactical LAN users transmitted during the 2nd and 4th time slots (15-30 & 45-00). The third time interval was allocated to Phoenix, an intelligence system. The division decided to use Frequency

Modulation (FM) radios for flash messages and have the Operations Officer (S3/G3) screen messages.

E. SECURITY

The biggest unresolved problem with TPN is security. There is a need for multiple levels of security on TPN, but it is a secret-high system. No other classification levels, i.e. unclassified, top secret, etc. can be used on TPN. This means that users with unclassified requirements can't send data across the net. This poses a problem for many TPN users, particularly the combat service support (CSS) community. The CSS users need to process both classified and unclassified traffic. Because of this shortfall, the CSS community is aggressively fielding a Mobile Gateway Van that will enable them to pass unclassified data on the battlefield and to the Defense Information Infrastructure.

There is no approved solution yet. However, one suggestion was to declassify the TPN backbone to the unclassified sensitive level and require secret and above hosts to implement end-to-end encryption (E3). Unclassified users would simply connect to the TPN. The encryption would segregate the unclassified and classified communities. Although there were several systems that could fulfill this need, Motorola's Network Encryption System (NES) was chosen as the preferred method. The Motorola NES has the advantage that it is already accredited by the National Security Agency (NSA) to process TOP SECRET data and below..

F. GATEWAY PROTOCOLS

1. Introduction

Not all of the TPN bandwidth challenges can be attributed to user actions. The Exterior Gateway Protocol (EGP) that TPN currently uses has enormous bandwidth requirements. The bandwidth requirements could increase drastically when DMS is implemented and routers are used on a large-scale basis.

There is another protocol, Border Gateway Protocol Version 4 (BGP-4) slated to replace EGP in 1997. This is a needed transition. However, to realize the value of the transition, it is important to understand what EGP is and the differences between EGP and BGP.

2. Exterior Gateway Protocol

a. Fat Protocol for Exterior Neighbors

EGP is the current standard protocol for external gateway communications in the Defense Data Network. It is the protocol that exterior neighbors use in the TPN. Two gateways that exchange routing information are said to be exterior neighbors if they belong to two different autonomous systems. They are called interior neighbors if they belong to the same autonomous system. EGP is the protocol that exterior neighbors use to advertise their reachability information to other autonomous systems.

EGP is considered a fat protocol because it requires that a neighbor advertise all reachability within its autonomous system with each update. Figure 20 depicted below illustrates how two exterior neighbors use EGP. Gateway 1 gathers information about the network in autonomous system 1 and reports the information to Gateway 2 via EGP. Gateway 2 does the same for its autonomous system and provides that information to Gateway 1.

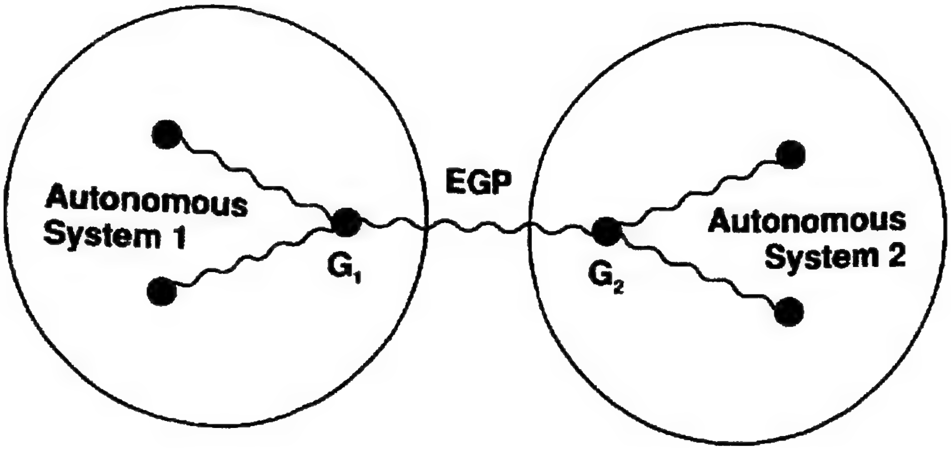


Figure 20. Exterior Gateway Protocol (EGP)
From [Ref. 12, p. 228]

b. EGP Message Categories

Exterior Gateway Protocol functionality contains three basic message categories. The first is that it contains a neighbor acquisition mechanism category that allows one gateway to request another to agree that the two should communicate reachability information. The second message category is the response category whereby a gateway continuously tests whether its EGP neighbors are responding. The last category is routing update. In the routing category, EGP neighbors periodically exchange network reachability information by passing routing update messages. Figure 21 below depicts the message categories, the message types and the corresponding descriptions.

MESSAGE CATEGORY	MESSAGE TYPE	DESCRIPTION
Neighbor Acquisition	Acquisition Request	Request gateway to become a neighbor (peer)
	Acquisition Confirm	Positive response to acquisition request
	Acquisition Refuse	Negative response to acquisition request
	Cease Request	Request termination of neighbor relationship
	Cease Confirm	Confirmation response to respond if alive
Response	Hello Request	Request neighbor to respond if alive
Testing/Reachablility	I Heard You	Response to hello message
Routing Update	Poll Request	Requests network routing update
	Routing Update	Network reachability information
	Error	Response to incorrect message

Figure 21. EGP Messages
From [Ref. 12, p. 228, Ref. 14, p. 19]

c. EGP Message Header

All EGP messages begin with a fixed header (see Figure 22) that identifies the message type. Each field has a unique purpose. The header field labeled Version tells what EGP version was used. Field type tells what type of message it is, and the code field helps distinguish among subtypes. The status field contains message-dependent status information and checksum verifies that the message was received in tact. The autonomous system num field provides the assigned number of the autonomous system of the gateway sending the message. The sequence number field contains a number that is used by the sender to synchronize messages and replies. When acquiring a neighbor, the gateway establishes an initial sequence value and increments the sequence number each time it sends a message. The neighbor replies with the last sequence number it received. This enables the sender to match responses to transmissions.

0	8	16	31
VERSION	TYPE	CODE	STATUS
CHECKSUM		AUTONOMOUS SYSTEM NUM.	
SEQUENCE NUMBER			

Figure 22. Fixed Header of EGP Messages
From [Ref. 12, p. 229]

d. EGP Neighbor Acquisition

- EGP Neighbor Acquisition Message: The manner in which EGP Neighbor Acquisition Messages occur is as follows. A gateway sends neighbor acquisition messages to establish EGP with another gateway. A key point is that EGP does not specify why or how one gateway chooses another gateway as its neighbor. Those choices are made by the organization responsible for administering the gateway, not via the software.

- EGP Neighbor Acquisition Header: The neighbor acquisition messages contain the standard header, initial values for a time interval to test whether the neighbor is alive (called a hello interval), and a polling interval. The polling interval controls the maximum frequency of routing updates. The sender supplies a polling interval indicating the limit of receiver polls, i.e., every n seconds, where n can be any number. The sender can change the time interval as needed. Also, the polling intervals can be asymmetric, allowing one peer to poll more frequently than the other.

- EGP Neighbor Reachability Information: There are two forms of testing whether a neighbor is alive in EGP. The first mode is the active mode, whereby gateways tell neighbors by periodically sending Hello messages in conjunction with poll messages and waiting for responses. In the passive mode, the gateway relies on its neighbor to periodically send hello or poll messages. It uses the information from the status field of a reachability message to determine whether the peer is alive or whether the peer knows it is alive. Normally both gateways in a pair operate in the active mode.

e. EGP Poll Request Messages

The EGP poll and request messages allow a gateway to obtain reachability information. There is an IP Source Network that specifies a network common to autonomous systems which both gateways attach. The response will contain routes that have distances measured with respect to gateways on the specified IP source network [Ref. 12, p. 232].

There are two important reasons that EGP makes a polling request to specify a source network. One is the gateway wants to connect to two or more physical networks. The other is if an application on the gateway implements EGP, it may not know over which interface EGP responses arrive. Hence, it may not know from which network the response comes. Also, gateways that run EGP often collect information for an entire autonomous system.

For autonomous systems, when advertising reachability, the exterior gateway sends neighbors a set of messages that specify a destination network in the autonomous system and the gateway used to reach that destination. Naturally, the gateway used to reach a destination depends on where traffic enters the autonomous system. The source network that is a part of the polling request message specifies the point at which packets will enter the autonomous system. Figure 23 illustrates the concepts of a common network used as a base for network reachability information.

f. EGP Routing Update Messages

The routing update message is used by an exterior gateway to convey information about reachable networks to its EGP neighbor. Usually, the gateway has already collected this information and is sharing the information with a gateway in another autonomous system. A gateway running EGP can report two types of reachability to a peer. The first report defines the destination networks that are reachable entirely within the gateway's autonomous system. The second report defines the gateways that it has learned about, but which lie beyond the gateway's autonomous system boundary.

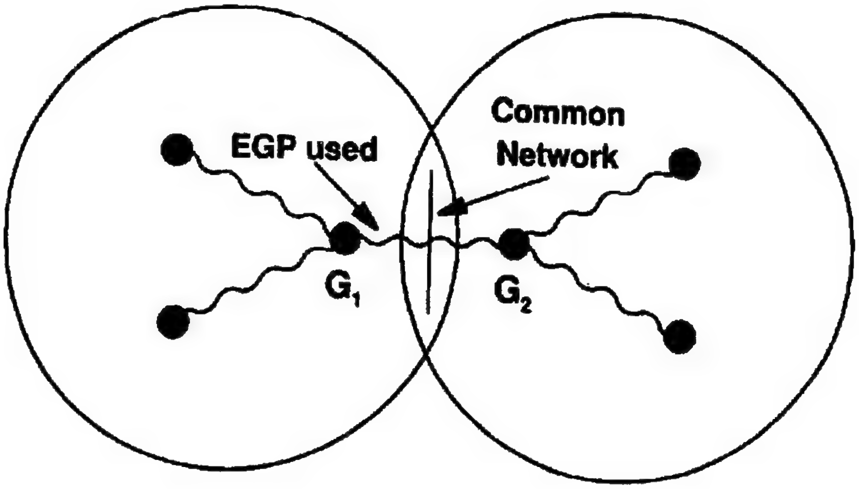


Figure 23. Network Reachability Information
From [Ref. 12, p. 233]

A noteworthy point is that EGP does not permit an arbitrary gateway to advertise reachability to an arbitrary destination network. It limits gateways to advertising only those destinations for which it is an authority. That is, EGP restricts a non-core gateway to advertise only those networks reachable entirely from within its autonomous system. The purpose of this rule, sometimes called the EGP third party restriction, is to control propagation of information and allow each autonomous system to choose how it advertises reachability.

G. BORDER GATEWAY PROTOCOL

1. Introduction

The Border Gateway Protocol is a newer more efficient way of exchanging exterior routing information. It is an inter-autonomous system routing protocol. An autonomous system (AS) is a set of routers under a single technical administration using an interior gateway protocol and common metrics to route packets within the AS, while using an exterior gateway protocol to route packets to other autonomous systems [Ref. 16].

2. BGP Efficiency

BGP is inherently more efficient than EGP, in that after an initial database exchange, only relatively small update messages are propagated for the duration of the neighbor relation. In other words, there is no need to refresh the entire routing table. The BGP messaging scheme contains four basic messages: OPEN, KEEPALIVE, NOTIFICATION, and UPDATE.

3. BGP Message Format

Every BGP message has a fixed size header. The data portion following the header is optional, depending on the message type. Figure 24 depicts the layout of the header fields. The marker is a 16-octet field that contains a value that the receiver of the message can predict. If the type of the message is OPEN, or if the OPEN message carries no authentication information, then the marker must be all ones. Otherwise, the marker value can be predicted by some computation specified as part of the authentication information used. The marker can also be used to detect loss of synchronization between a pair of BGP peers, and to authenticate incoming BGP messages.

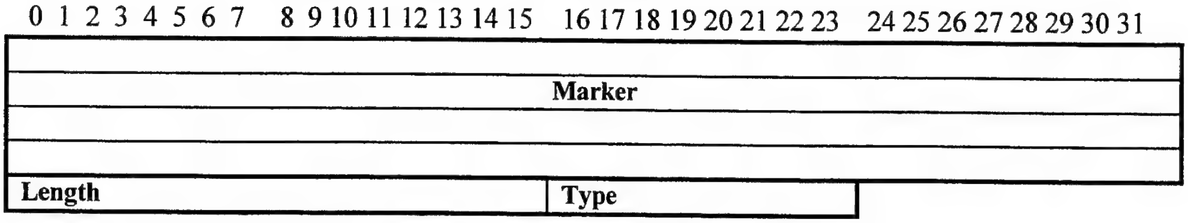


Figure 24. Message Header Format
After [Ref. 16, p.6]

a. Length Field

The length field is a 2-octet unsigned integer. It indicates the total length of the message, including the header, in octets. The value of the length field must always be at least 19 and no greater than 4090. It may be further constrained depending on the message type. Since no "padding" of extra data after the message is allowed, the length field must have the smallest value required given the rest of the message.

b. Type Field

The type field is a 1-octet unsigned integer that indicates the code type of the message. The code types defined correspond to the four types of messages: OPEN, UPDATE, NOTIFICATION, and KEEPALIVE.

4. The OPEN Message

The first message sent by each side, after a transport protocol is established is an OPEN message. The OPEN message is used to solicit/establish a BGP relationship with a neighbor and transfers initial configuration information. The information includes: the BGP version number, the local AS number, the IP address of the BGP speaker soliciting the neighbor relationship, and the maximum time that can elapse between KEEPALIVE messages before the neighbor will be declared "down" (resulting in all routes associated with that neighbor being deleted from the database) [Ref. 14]. The OPEN message also contains an authentication code along with associated data which allows a BGP neighbor request to be authenticated. Once the OPEN message is confirmed, UPDATE, KEEPALIVE and NOTIFICATION messages may be exchanged.

5. The KEEPALIVE Message

A KEEPALIVE message is used to send back a message to the originator confirming that the OPEN message was acceptable. The 19 byte KEEPALIVE message is transmitted periodically between peers to maintain a neighbor relationship. The OPEN message specifies the maximum time (hold time) that can elapse between KEEPALIVE messages before a neighbor connection is considered closed. The KEEPALIVE message interval is generally set to one third of the maximum hold-time interval to maintain the neighbor relationship.

6. The NOTIFICATION Message

A NOTIFICATION message is sent only when an error condition is detected. If a connection encounters an error connection, a NOTIFICATION message is sent and the connection is closed. Closing a BGP connection implies that the transport protocol has been closed and that all resources for that BGP connection have been deallocated. The NOTIFICATION message contains the Error Code, the Error Subcode, and Data Fields.

7. The UPDATE Message

An UPDATE message is used to transfer routing information between BGP peers. The message is used to advertise a single feasible route to a peer or to withdraw multiple unfeasible routes from service. All BGP messages contain the standard header. The UPDATE field can include the other fields reflected shown in Figure 25.

0 --7 8--15

Unfeasible Routes Length in bytes (2 Bytes)

Withdrawn Routes (Variable Length)

IP Prefix Length for Withdrawn Route in Bits	IP ------------------Prefix ------------------
------------------8/16/24/32 Bits --------	-------- -------------

Total Path Attributes Length in Bytes (2 Bytes)

Path Attributes (Variable Length)

<Attribute Type, Attribute length, Attribute Value>	

Network Layer Reachability Information (Variable Length)

IP Prefix Length for Route in bits	IP ------------------Prefix ------------------
------------------------8/16/24/32 Bits --------	---------------------

Figure 25. BGP Header
From [Ref. 14, p. 33]

- Unfeasible Routes Length (2 Octets)
- Withdrawn Routes (variable)
- Total Path Attributes Length (2 Octets)
- Path Attribute (variable)
- Network Layer Reachability Information (variable)

The unfeasible routes length provide the total length of the withdrawn route in bytes. The value must allow the length of the Network Layer Reachability Information field to be determined. For example, a value of zero means that no routes are being withdrawn from service. Therefore, the Withdrawn Routes field is omitted in the UPDATE message. As the name implies, withdrawn routes contain a list of IP address prefixes for the routes that are being withdrawn from service. The total path attributes length indicates the total length of the Path Attribute field in octets. Like the unfeasible router length, its value must allow the length of the Network Layer Reachability Field to be determined. A value of zero in the Total Path Attribute Field indicates that no Network Layer Reachability Information field is present.

Every update contains a variable length sequence of path attribute. The path attribute is three parameters of variable length. They are: attribute, value, and attribute length.

The Network Layer Reachability Information field identifies the IP prefixes of all networks that can be reached via the defined path. The message format for identifying these networks is the same as the format for "withdrawn routes"

H. COMPARISON OF BGP AND EGP

Since BGP is a more modern protocol, it is not surprising that the benefits gained by upgrading from EGP to BGP outweigh the disadvantages, if any. The key benefit is because of the bandwidth savings. Tests have been conducted that revealed that the use of BGP approximately halves the required bandwidth consumption on the narrow (16 kbps) NC to SEN link. Additionally, BGP offers increased routing flexibility. As an example, a non-core gateway speaking EGP will advertise only networks reachable entirely from within the gateway's autonomous system. The BGP-4 implementations contain no such limits.

When providing updates, BGP propagates only changes to neighbors, thus inherently, it consumes less bandwidth. EGP, on the other hand sends a full database update every 3-5 minutes. Additionally, BGP provides flexibility for TPN. Since DDN is already being converted to BGP, some of the interoperability problems can be alleviated.

Table 1 depicts the significant BW benefit of BGP over EGP based on simulations conducted by GTE. In every category, BGP consumed less BW except for the average link between the NCS and LEN. The reason is that in the EGP scenario global routing information is not downloaded to local routers.

Table 1. Highlights of Current EGP Approach

From [Ref. 14, p. 42]

	Current EGP	**Recommended BGP Approach**
% bandwidth consumed on the 64 kbps NCS to NCS links in the MPN backbone		
Worst link in network	51.5%	9.7% (NCS20 to NCS 16)
Average link	12.7%	4.9%
Worst case % bandwidth consumed on T/20 to T/20 link across MPN IP Boundary	38.6%	3.2%
% bandwidth consumed on the 16 kbps link between each NCS and SEN		
Worst link in network	8.0%	4.5%
Average link	1.9%*	4.5%
% bandwidth consumed on the 56 kbps link between each T/20 and its local C3/X(A) Packet Switch		
Worst link in network	90.2%	9.7%
Average link	7.3%	6.3%

*In EGP scenario, global routing information was not downloaded to local routers. Rather, each router had to configure a default route to the T/20. The global routing information is downloaded to the routers in the BGP scenario, and the configuration of default routes is not required.

VI. EVOLVING COMMUNICATIONS REQUIREMENTS

A. THE NEW STAGE

Thus far, this thesis has focused on a service-unique system with organic issues and concerns. It is important to resolve service initiatives first. However, this is a near-sighted view that continues to fade. Based upon operations other than war, i.e., peacekeeping exercises conducted in Somalia and Haiti, the stage is set for a new way of thinking and implementation. The new stage is a joint one that is not likely to digress or revert back to single service perspectives. Therefore, the U.S. Army must plan accordingly.

B. PLANNING FOR JOINT CHALLENGES

The United States Army Signal Center and Fort Gordon (USASC&FG) recognizes this new perspective and has modified communication lesson plans. While the Signal Community still teaches service doctrine and service-unique systems, the emphasis has shifted. The school is emphasizing that unless a training exercise is conducted in your own back yard (training area), it will be a joint operation. Thus, students are introduced to the joint planning process. Joint planning is vital to meeting the evolving joint communication requirements.

Planning is thinking of every possible requirement before deployment; whilst one can always locally purchase an electrical plug or a computer, without prior planning, it is unrealistic to ask for and expect a 512 kbps link via WESTLANT satellite tomorrow [Ref. 17]. A key component of planning is the mission statement. It kicks off the entire planning process. However, since the mission statement can be generic, i.e., provide communications for Joint Task Force (JTF) Bravo, the planner must seek to find out who, where, what, how, and so forth.

The "who" used to be very simple, but now the users are many and varied. The list could include:

- Component Forces
- Special Operation Forces
- The American Embassy
- The Host Nation
- Allied Forces
- Miscellaneous Users
- The Post Exchange
- The Red Cross
- The Media

The type of service the users require falls in to three basics groups: voice, record traffic, and data. The subsets of these groups are provided in Table 2.

Table 2. Services Provided

Voice:	Secure Common User (ACUS)	
	Portable Off the Shelf (POTS)	
	Defense Switched Network (DSN)	
	Point-to-point Hotline	
Record Traffic:	Automated Digital Network (AUTODIN)	
	Tactical (AN/TYC-39)	
	Fax (AN/UXC-15)	
Data	Networks	Tactical
		Strategic
	Applications	Weather

C. PRINCIPLES OF PLANNING

The communication plan to provide the services reflected above must be derived from a number of principles. Army signal officers attending doctrinal schools: Signal Officer Basic Course (SOBC) and Signal Officer Advance Course (SOAC) are taught nine principles of planning. The principles, when employed, facilitate the planning process.

1. Interoperablility

Considering the evolving communication requirements in a joint arena, interoperability is the first and most important principle of communications. Frank M. Snyder, author of *Command and Control*, defines interoperability as, "The condition achieved among communications-electronics systems (CE) or items of CE equipment when information or services can be exchanged directly and satisfactorily between them and/or their users [Ref. 18, p. 110].

In simplistic terms, interoperability is the condition achieved among command, control, communications and computers (C4) systems or C4 equipment when information or services can be exchanged. Though expressed in simplistic terms, the implementation of this principle is complex.

Interoperability encompasses: (1) acquisition and employment of interoperable systems, (2) development and enforcement of interoperability standards, and (3) the training of personnel. This principle (interoperability) is the one most cited in after-action reviews as a continuing problem [Ref. 17].

2. Discipline

Discipline is the second principle. Discipline is the ability to control the flow of information gathering, processing, directing, and reporting to the commander. The goal is to restrict the flow of information to the commander to his needs, nothing more. Standardized reporting formats, standardized databases, structures, and other physical or procedural measures can be used to limit the flow. The C4I for the Warrior smart-push, warrior-pull idea is an example of this concept [Ref. 17].

3. Economy

The third principle of communication is economy. Economy in employment should not be misconstrued as eliminating alternative routes that were deliberately designed into the communication system. The purpose of economizing is to eliminate unnecessary redundancy by consolidating assets wherever possible.

4. Flexibility

All C4 systems must have flexibility in this rapidly changing joint environment. The system manager must be able to react to unexpected challenges to ensure the continuity of communications support. To ensure the C4 system is flexible, the planner should consider: providing for alternate routes, preplanning alternate positions for communication sites, planning alternate frequencies, and other techniques.

5. Security

Although security is the fifth principle, it is an issue that must be addressed as early as possible. The level of communications security required for a given link or system must be determined during the network design phase.

6. Reliability

A communication system is often judged based on how reliable it is. If the one instance that the commander attempts to use the system, it fails, the system reliability is a problem. The commander must be able to rely on the availability of the system. Reliability is achieved during the design phase of the equipment and during the engineering of the equipment.

7. Survivability

One of the military unique "ilities" is survivability. As the information revolution continues to evolve, so should concern about information operations or information warfare. Survivability encompasses the ability to resist detection and jamming, the ability to survive the effects of electromagnetic pulse, and other aspects of information warfare. The planner cannot overlook the survivability principle.

8. Timeliness

Perhaps the most essential principle in the minds of commanders is timelines. Timeliness includes installation times and transmission times. The time criticality of certain intelligence and operations require rapid transmission of data over the system. This requirement affects both the size of the circuits and the prioritization process. Timeliness is key to the planning process because old intelligence can be worst than no intelligence.

9. Combined Operations

The evolution of communication requirements extend not only to the joint environment, but to the coalition environment as well. These combined operations involve the previous eight principles discussed along with the five listed below.

- Standardization of principles
- Agreements in advance of war
- Establishment of policy in the absence of an agreement
- Use of U.S. interpreters, and
- Choice of cryptographic systems.

The standardization of principles and agreements in advance of war are well-established in alliances like the North Atlantic Treaty Organization (NATO). However, few if any exist in coalitions. Therefore, policies may have to be established to ensure interoperability. Liaison teams and interpreters are critical to the success in terms of interfacing and control of the communication system

The choice of cryptographic systems add more complexity to combined operations. Even if the communication systems are completely interoperable, the issue of which Communications Security (COMSEC) devices are authorized for use by foreign nations and which are for U.S. use only can be very difficult to resolve [Ref. 17]. The communications planner must be cognizant of this critical issue and its impact upon achieving the principles of communication.

D. THE FUTURE PATH

The question of "Where do we go from here?" is difficult to answer considering the changing global structure and the restructuring of the U. S. Armed Forces. The fall of the Soviet Union resulted in a strategy change. We know that we have a new enemy. We know that we should be prepared to fight two enemies on different fronts simultaneously. We also know that we must have a paradigm shift as we posture forces for the challenges of the 21st Century. Equally important, we must have a framework for future communications.

1. The Army Enterprise Strategy

The Army Enterprise Strategy is a single, unified vision for the Army C4I community that serves as the framework by which the U.S. Army will meet and conquer the joint interoperability challenges of the 21st Century [Ref. 17]. The Enterprise Strategy is manifested in two publications: *The Vision* and *The Implementation Plan. The Vision* is an aggregate of ten principles aimed at ensuring that the warfighter will have information superiority over any opponent. *The Implementation Plan* reflects the actions required to fulfill the vision.

a. The Vision

The Vision is a masterful publication in that it truly captures the essential requirements to support the warfighter. The bullets below reflect the ten principles of the vision. The publication *The Vision,* provides some of the implicit and implied tasks associated with the principles [Ref. 17].

- Focus on the Warfighter - Provide the Warfighter C4I systems that meet validated needs.
- Ensure Joint Interoperability - Provide the Warfighter C4I systems that interoperate in Joint and Combined operations.
- Capitalize on Space-Based Assets - Provide the Warfighter assured access to mission essential military and commercial space-based systems that support the Force Projection Army across the entire operational continuum.
- Digitize the Battlefield - Provide the Warfighter an integrated digital information network that supports warfighting systems and assures C2 decision-cycle superiority.
- Modernize Power Projection Platforms - Provide the Warfighter a modern power projection platform to support peacetime operations, mobilization, force projection, split-base operations, and redeployment.

- Optimize the Information Technology Environment - Provide the Warfighter with more efficient information support for combat and peacetime operations.

- Implement Multi-Level Security - Provide the Warfighter the ability to access and exchange information at needed levels of classification using a single C4I system.

- Acquire Integrated Systems Using Commercial Technology - Provide the Warfighter C4I capabilities that leverage commercial technology.

- Ensure Spectrum Supremacy - Provide the Warfighter electromagnetic spectrum supremacy in order to maximize the benefits of maneuver and tempo in conjunction with firepower.

b. The Implementation Plan

The framework for the future must be realized by actions to achieve the vision. The Army Enterprise Strategy Implementation Plan represent the actions required to prepare the U.S. Army for the challenges of the 21st Century. The evolution and modernization of Army C4I systems are key aspects of the plan. The plan provides further definition and insight of the Vision document, outlines a high-level C4 migration blueprint, directs nine implementation tasks, and defines a management structure [Ref. 20].

Before the future course can be charted, the current course must be recognized or identified. *The Implementation Plan* not only provides a self-assessment in terms of where we are now; it goes a step further by stating where we want to go and how we intend to get there. It reflects that the U.S. Army has made a paradigm shift from a focus shaped by the forward deployment of forces and equipment to a focus forged by force projection.

The paradigm shift must be reflected in our C4I strategy. Table 3 reflects an information-technology-based paradigm shift.

2. Warfighter Information Network (WIN)

One of the most recent communications schemes reflect the new way of thinking. It is a plan that envisions a Warrior Information Network. The goal of the WIN is to design an architecture that will support Force XXI well into the 21st Century with leap-ahead technology that allows simultaneous voice, data, and video communications service on a single channel at all levels of security [Ref. 21].

Table 3. Shifting Paradigms

Old Model	New Concepts/Technology	New Model
Forward Deployed	Force Projection	Installation is Division, Corps Rear Area
Service Focused Information	Joint Operations	Joint and Combined Information
Deploy Extensive IM Systems in Theater	Satellite, Packet Switching, PC power	Send Only Terminals, Limited Hubs Forward
Hardware Dominant Weapons Systems	Computer Technology, Software Engineering	Software Enables Combat Power
Focus on Weapons Systems, Time, Space	Real Time Information Distribution	Information Warfare
Umbrella Communications Grid	Force Mobility	Support Cells and Selected Areas, Use Range Extension
Acetate and Grease Pencil	Fiber, Space, ATM, Automation	Imagery, Simulation, Electronic Map Displays, Print Locally When Required
Stove Pipe Systems	Distributed Data Base	Process Oriented IMA Support
Manual Serial Coordination	Groupware	Electronic Coordination
Print Plants with Multi Step Process	Direct Publishing Access	Electronic Preparation and Distribution
Military Unique IMA Equipment	High Technology Changes in:	
	Commercial Switches	CCITT Standard Commercial Switches
	Open System Environment	Commercial equipment Software independent of hardware. Tech insertion independent or together
	Photography	Cameras authorized Transmit to Multimedia Ops Center use
	Commercial Space Transmission and Switching	Augment Minimum Essential Military with Commercial or start with COTS and modify as needed

The WIN plan takes advantage of the latest technology, i.e., Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN), and Synchronous Optical Network (SONET). Under the WIN concept, current communications equipment will be replaced. The ATM switch will replace the NC and LEN switches. The Future SEN (FSEN) will replace current SENs (both versions), increasing the throughput range dramatically by supporting moderate bandwidth speeds of 64 kbps to 1.544 megabits per second (mbps). Current LOS radios will be replaced by High Capacity Trunk Radios, capable of a minimum data rate of 45 mbps to support the ATM switching. This bold plan will result in communications enhancements for all subscribers, including Video Teleconferencing (VTC) subscribers. It resolves the bandwidth challenges of today and modernizes communications by using emerging technologies. The WIN provides an excellent framework to support the evolving communication requirements.

3. Conclusion

> The ability to rapidly gather, manage, and distribute information will provide a decisive advantage on the 21st Century battlefield. Individual programs are important, but even more important is the synergistic effect of the incorporation of information technology across our systems. As we insert digital technology into our battlefield systems, we are building an Army of unprecedented capability.
>
> General Gordon Sullivan, Chief of Staff , U.S. Army (CSA)

The statement above summarizes the Army's future perspective. TRADOC Pamphlet 525-5 represents future concepts or ideas for 21st Century Army Operations. A key point it makes is that there must be a revolution in military affairs (RMA). We must continue to have innovations in technology and we must change our doctrine as needed. Additionally, we must not forget to maintain the soldier focus. Simply stated, our future Army will continue to recognize the soldier as its greatest asset and build our future operational concept around quality soldiers and leaders. [Ref. 22 p. 3-24].

Clearly, the evolving communication requirements mandate that the U.S. Army be prepared to operate in a joint environment. Therefore, it is critical for planners to know and use the nine principles of planning. Interoperability and coalition issues will continue to foster new challenges. Having a blueprint available will certainly make the process easier. The blueprint must, however, extend beyond joint operations and reflect future expectations. The Army Enterprise Strategy addresses these future challenges. The WIN is key to fulfilling the concepts envisioned.

VII. CONCLUSION

A. INTRODUCTION

The principal aim of this thesis was to look at GTE's proposal to provide enhancements to the U.S. Army Tactical Packet Network (TPN). This included an analysis of current communication capabilities, packet switching concepts, unresolved issues, and the future direction of the U.S. Army with regard to C4I. The results of this thesis are based on analysis of the technological solutions chosen, an extensive review of TPN after-action reports (AARs), and a close analysis of the Army's long term C4I strategy.

B. THESIS RESULTS

The current transmission rate for Army tactical communications equipment is not high enough to support the anticipated bandwidth requirements of the digitized battlefield [Ref. 21]. Therefore, the Army must use the latest solutions that technology offers. The Warfighter Information Network (WIN) design employs a modern solution. The architecture reflects usage of ATM and ISDN technology. But ATM has a minor drawback that must be overcome. ATM performs limited error detection operations [Ref. 23]. Consequently, line-of-sight and satellite systems with high Bit Error Rates (BER) could cause problems.

The Army's plan must meet the needs of the warfighter and reflect a joint focus for the new environment. Furthermore, the plan should encapsulate future requirements by taking a long view. Peter Schwartz, author of *The Art of the Long View,* suggests that scenarios are tools for helping us take a long view in a world of great uncertainty [Ref. 24]. The U.S. Army's long view is reflected in the Army Enterprise Strategy. Part of the warfighter focus contained within the strategy includes implementation of Battle Lab Concepts to look at different scenarios via simulations.

The GTE proposal is the best solution to resolve the current TPN shortfalls. It takes advantage of the latest gateway protocol technology and is somewhat far-sighted in that it addresses the anticipated interoperability issue regarding DMS and TPN. However, the proposal is not the optimal solution. The optimal solution would have to capitalize on the latest technological equipment. Unfortunately, this is easier said than done. The U.S. Army can not shut down to retrofit or replace existing communications. Besides, based on evolving system life cycles, by the time the upgrade was completed, a newer system would be available.

Given the budgetary constraints and the need to keep pace with technology, there are no easy alternatives when trying to decide whether to upgrade or replace an existing system. The best solution could be to have a feasible plan. The TPN upgrade plan is feasible to ameliorate immediate challenges, and the nine principles of planning provide the requisites for joint communications. Additionally, the Army Enterprise Strategy represents a sound approach to meet future requirements. It is a masterful document containing a vision that is goal-oriented and an implementation plan that is action-oriented. The strategy reflects several elements of the organizational infrastructure for implementing total quality management (TQM). However, the key to the Army Enterprise Strategy's success is the seventh element of TQM. The implementation effort must be monitored and diagnosed by top management [Ref. 25].

C. FURTHER RESEARCH

Further research efforts could analyze the various methods or options to perform multilevel security. The U.S. Army Signal Center recently submitted an operational requirement document (ORD) to seek approval to use Motorola's Network Encryption System (NES) for TPN customers. Although NES is the preferred solution, there could be other options available. Another area worth investigating is the application of Low Earth Orbit Satellites (LEOs) for Department of Defense or service-unique missions. LEOs are a new and emerging technology that are not yet reflected in future architectural designs.

LIST OF REFERENCES

1. Aspin, Les, "The Bottom-Up Review: Forces For A New Era," Department of Defense, September 1, 1993.

2. Naisbitt, John, *Megatrends*, New York: Warner Books, 1982.

3. Coakley, Thomas P., *Command and Control for War and Peace*, Washington, D.C.: National Defense University Press, 1992.

4. *Army Tactical Command and Control System (ATCCS) Systems Management Techniques, FM-7,* Washington, D.C., Department of the Army, 1993.

5. *Area Common User System (ACUS) Reference Guide*, Ft. Monmouth, New Jersey, U.S. Army, Project Manager, Joint Tactical Area Communications Systems, n.d.

6. Fitzgerald, Jerry, *Business Data Communications,* Fourth Edition, New York: John Wiley & Sons, 1993.

7. Rosner, Roy D., *Packet Switching*, Belmont, California: Lifetime Learning Publications, 1982.

8. Judge, Peter, *Open Systems*, Wellesley, Massachusetts: QED Information Sciences, 1988.

9. *Tactical Packet Network (TPN)/Command Post (CP) Architecture Interconnectivity Study Report (DRAFT)*, Washington, D.C.: GTE Government Systems for the Department of the Army, 1994.

10. *TPN Handbook (2nd Draft)*, U.S. Army, Project Manager, Joint Tactical Area Communications Systems, 1994.

11. *Tutorials on Global Network Intelligence Topics,* Delran, New Jersey: Datapro, 1989.

12. Comer, Douglas E., *Internetworking with TCP/IP, Volume I*, Englewood Cliffs, New Jersey: Prentice Hall, 1991.

13. "February 1994 TNMC Trip Report," Memorandum for Commander 22d Signal Brigade, February 18, 1994.

14. *MPN IP Router Study Final Report,* GTE Systems Engineering, December 1993.

15. "11 February 1994 V Corps NAG Minutes," Minutes From Commander, 22nd Signal Brigade, 11 February 1994.

16. "rfc1771," Memo, Network Working Group, March 1995.

17. "Lesson Plan F02-LP1," U.S. Army Signal Center and Fort Gordon, Fort Gordon, Georgia, Lesson Plan, April 1996.

18. Snyder, Frank M., *Command and Control*, Washington, D.C.: National Defense University Press, 1993.

19. *The Vision*, Office of the Secretary of the Army, Washington, D.C., 1993.

20. *The Army Enterprise Implementation Plan*, Washington, D.C.: Department of the Army, 1994.

21. Loop, Tony L., "Warfighter Information Network and the Next Generation of Switches," Paper, U. S. Army, 5 July 1995.

22. *TRADOC Pamphlet 525-5*," Department of the Army, Fort Monroe, Virginia, 1 August 1991.

23. Black, Uyless, *Emerging Communications Technologies*, Englewood Cliffs, New Jersey: Prentice Hall, 1994.

24. Schwartz, Peter, *The Art of the Long View*, New York: Doubleday, 1991.

25. Shiba, Shoji, Alan Graham, and David Walden, *A New American TQM Four Practical Revolutions In Management*, Portland, Oregon: Productivity Press, 1993.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Dudley Knox Library Naval Postgraduate School 411 Dyer Rd. Monterey, California 93943-5101	2
3.	Professor Gilbert M. Lundy Code CS/Ln Naval Postgraduate School Monterey, California 93943-5101	1
4.	Professor Orin E. Marvel Code CC/Ma Naval Postgraduate School Monterey, California 93943-5101	1
5.	Program Executive Office-Communications Systems SFAE-CM/SFAE-CM-JTC-TMD Don Keller Ft. Monmouth, New Jersey 07703	1
6.	Earnest E. Hansley 106 Dexter St. Vidalia, Georgia 30474	3
7.	Professor Dan C. Boger Code CC Naval Postgraduate School Monterey, California 93943-5101	1